Kaspersky Anti-Virus 2011 for Mac

Benutzerhandbuch

PROGRAMMVERSION: 8.0.6

Sehr geehrter Benutzer!

Vielen Dank, dass Sie unser Produkt ausgewählt haben. Wir hoffen, dass dieses Dokument Ihnen in Ihrer Arbeit hilft und die meisten aufkommenden Fragen beantworte.

Wichtiger Hinweis: Die Rechte an diesem Dokument liegen bei der Kaspersky Lab GmbH und sind durch die Urhebergesetze der Russischen Föderation und durch internationale Abkommen geschützt. Bei illegalem Vervielfältigen und Weiterverbreiten des Dokuments oder einzelner Teile daraus kann der Beschuldigte nach geltendem Recht zivilrechtlich, verwaltungsrechtlich und strafrechtlich zur Verantwortung gezogen werden.

Das Vervielfältigen in jeglicher Form und das Weiterverbreiten, unter anderem auch in übersetzter Form, aller Unterlagen ist nur nach vorheriger schriftlicher Genehmigung der Kaspersky Lab GmbH zulässig.

Das Dokument und die dazugehörigen Grafiken dürfen nur zu informativen, nicht kommerziellen und persönlichen Zwecken verwendet werden.

Änderungen des Dokuments ohne vorherige Ankündigung bleiben vorbehalten. Die jeweils neueste Version des Dokuments finden Sie auf der Webseite von Kaspersky Lab unter der Adresse http://www.kaspersky.com/de/docs.

Kaspersky Lab ZAO übernimmt keine Haftung für den Inhalt, die Qualität, die Aktualität und Richtigkeit der im Dokument verwendeten Unterlagen, die das Eigentum anderer Rechtsinhaber sind, sowie für den möglichen Schaden durch die Nutzung dieser Unterlagen.

In diesem Dokument werden eingetragene Markenzeichen und Handelsmarken verwendet, die das Eigentum der jeweiligen Rechtsinhaber sind.

Erscheinungsdatum: 20.12.2010

© 1997-2010 Kaspersky Lab ZAO. Alle Rechte vorbehalten.

http://www.kaspersky.com/de/
http://support.kaspersky.com/de/

LIZENZVEREINBARUNG

WICHTIGER RECHTLICHER HINWEIS AN ALLE NUTZER: LESEN SIE FOLGENDE RECHTLICHE VEREINBARUNG SORGFÄLTIG DURCH, BEVOR SIE DIE SOFTWARE NUTZEN.

INDEM SIE IM LIZENZVERTRAG-FENSTER AUF DIE SCHALTFLÄCHE AKZEPTIEREN KLICKEN ODER EIN ENTSPRECHENDES ZEICHEN BZW. ENTSPRECHENDE ZEICHEN EINGEBEN, ERKLÄREN SIE SICH MIT DER EINHALTUNG DER GESCHÄFTSBEDINGUNGEN DIESES VERTRAGS EINVERSTANDEN. **DIESE AKTION KONSTITUIERT EIN BEKENNTNIS IHRER SIGNATUR UND SIE STIMMEN DIESER VEREINBARUNG, UND DASS SIE EINE PARTEI DIESER VEREINBARUNG WERDEN, ZU UND ERKLÄREN SICH WEITERHIN EINVERSTANDEN, DASS DIESE VEREINBARUNG, WIE JEDWEDE ANDERE SCHRIFTLICHE, AUSGEHANDELTE UND DURCH SIE UNTERZEICHNETE VEREINBARUNG AUCH, VOLLSTRECKBAR IST.** SOLLTEN SIE MIT DEN GESCHÄFTSBEDINGUNGEN DIESER VEREINBARUNG NICHT EINVERSTANDEN SEIN, BEENDEN SIE DIE INSTALLATION DER SOFTWARE BZW. INSTALLIEREN SIE SIE NICHT.

NACHDEM SIE IM LIZENZVERTRAG-FENSTER AUF DIE SCHALTFLÄCHE AKZEPTIEREN GEKLICKT ODER EIN ENTSPRECHENDES ZEICHEN BZW. ENTSPRECHENDE ZEICHEN EINGEGEBEN HABEN, SIND SIE BERECHTIGT, DIE SOFTWARE IM EINKLANG MIT DEN GESCHÄFTSBEDINGUNGEN DIESER VEREINBARUNG ZU NUTZEN.

1. Definitionen

1.1. **Software** bezeichnet Software einschließlich aller Updates und zugehöriger Materialien.

1.2. **Rechtsinhaber** (Inhaber aller Rechte an der Software, ob exklusiv oder anderweitig) bezeichnet Kaspersky Lab ZAO, ein gemäß den Gesetzen der Russischen Föderation amtlich eingetragenes Unternehmen.

1.3. **Computer** bezeichnet/bezeichnen Hardware, einschließlich von PCs, Laptops, Workstations, PDAs, Smart Phones, tragbaren oder sonstigen elektronischen Geräten, für welche die Software konzipiert war und auf denen die Software installiert und/oder verwendet werden wird.

1.4. **Endnutzer (Sie)** bezeichnet eine bzw. mehrere Personen, die die Software in eigenem Namen installieren oder nutzen, oder die eine Software-Kopie rechtmäßig nutzt/nutzen, oder, falls die Software im Namen einer Organisation heruntergeladen oder installiert wurde, wie etwa einem Arbeitgeber, bezeichnet der Begriff *„Sie“* weiterhin jene Organisation, für die die Software heruntergeladen oder installiert wird, und es wird hiermit erklärt, dass eine solche Organisation die diese Vereinbarung akzeptierende Person autorisiert hat, dies in ihrem Namen zu tun. Im Sinne dieses Lizenzvertrags beinhaltet der Begriff *„Organisation“* ohne Einschränkungen jedwede Partnerschaft, GmbH, Gesellschaft, Vereinigung, Aktiengesellschaft, Treuhandgesellschaft, Gemeinschaftsunternehmen, Arbeitsorganisation, nicht eingetragene Organisation oder staatliche Behörde.

1.5. **Partner** bezeichnet Organisationen oder Personen, die die Software auf Grundlage eines Vertrags und einer mit dem Rechtsinhaber vereinbarten Lizenz vertreiben.

1.6. **Update(s)** bezeichnet/n alle Upgrades, Korrekturen, Patches, Erweiterungen, Reparaturen, Modifikationen, Kopien, Ergänzungen oder Wartungs-Softwarepakete usw.

1.7. **Benutzerhandbuch** bezeichnet die Bedienungsanleitung, die Administrator-Anleitung, ein Nachschlagewerk und ähnliche erläuternde oder sonstige Materialien.

2. Lizenzgewährung

2.1. Der Rechtsinhaber gewährt Ihnen hiermit eine nicht-ausschließliche Lizenz zur Speicherung, zum Laden, zur Installation, Ausführung und Darstellung (zur „Nutzung“) der Software auf einer festgelegten Anzahl von Computern zur Unterstützung des Schutzes Ihres Computers, auf dem die Software installiert ist, vor im Nutzerhandbuch beschriebenen Bedrohungen gemäß den technischen, im Benutzerhandbuch beschriebenen Anforderungen und im Einklang mit den Geschäftsbedingungen dieses Vertrags (die „Lizenz“). Sie erkennen diese Lizenz an.

Testversion. Sollten Sie eine Testversion der Software erhalten, heruntergeladen und/oder installiert haben und sollte Ihnen hiermit eine Evaluierungslizenz für die Software gewährt worden sein, dürfen Sie die Software ab dem Datum der ersten Installation nur zu Evaluierungszwecken verwenden, und zwar ausschließlich während der einzigen geltenden Evaluierungsperiode, außer wie anderweitig angegeben. Jegliche Nutzung der Software zu anderen Zwecken oder über die geltende Evaluierungsperiode hinaus ist strikt untersagt.

Software für mehrere Umgebungen; Mehrsprachige Software; Dual-Medien-Software; Mehrere Kopien; Softwarebündel. Wenn Sie verschiedene Versionen der Software oder verschiedene Sprachausgaben der Software verwenden, wenn Sie die Software auf mehreren Medien erhalten, wenn Sie anderweitig mehrere Kopien der Software erhalten oder wenn Sie die Software mit einer anderen Software gebündelt erhalten sollten, entspricht die insgesamt zulässige Anzahl Ihrer Computer, auf denen alle Versionen der Software installiert sind, der Anzahl der Computer, die in den Lizenzen festgelegt ist, die Sie vom Rechtsinhaber bezogen haben, und jede erworbene Lizenz berechtigt Sie zur Installation und Nutzung der Software auf dieser Anzahl von Computern entsprechend den Festlegungen in den Klauseln 2.2 und 2.3, *außer die* Lizenzbedingungen sehen eine anderweitige Regelung vor.

2.2. Wenn die Software auf einem physischen Medium erworben wurde, haben Sie das Recht, die Software zum Schutz einer solchen Anzahl von Computern zu verwenden, die auf der Softwareverpackung festgelegt ist.

2.3. Wenn die Software über das Internet erworben wurde, haben Sie das Recht, die Software zum Schutz einer solchen Anzahl von Computern zu verwenden, die genannt wurde, als Sie die Lizenz für die Software erworben haben.

2.4. Sie haben das Recht, eine Kopie der Software anzufertigen, und zwar ausschließlich zu Sicherungszwecken und nur, um die rechtmäßig in Ihrem Besitz befindliche Kopie zu ersetzen, sollte eine solche Kopie verloren gehen, zerstört oder unbrauchbar werden. Diese Sicherungskopie kann nicht zu anderen Zwecken verwendet werden und muss zerstört werden, wenn Sie das Recht verlieren, die Software zu nutzen oder wenn Ihre Lizenz abläuft oder aus irgendeinem Grund im Einklang mit der gültigen Gesetzgebung im Land Ihres Wohnsitzes oder in dem Land, in dem Sie die Software nutzen, gekündigt werden sollte.

2.5. Sie können die nicht-exklusive Lizenz zur Nutzung der Software an andere Personen innerhalb des Rahmens der Ihnen vom Rechtsinhaber gewährten Lizenz übertragen, vorausgesetzt, dass der Empfänger allen Geschäftsbedingungen dieses Vertrags zustimmt bzw. bejaht, Sie vollständig in der vom Rechtsinhaber gewährten Lizenz zu vertreten. In dem Fall, dass Sie die vom Rechtsinhaber gewährten Rechte zur Nutzung der Software vollständig übertragen, müssen Sie alle Kopien der Software, und zwar einschließlich der Sicherungskopie, zerstören. Wenn Sie Empfänger einer übertragenen Lizenz sind, müssen Sie zustimmen, alle Geschäftsbedingungen dieses Vertrags einzuhalten. Wenn Sie den Geschäftsbedingungen dieses Vertrags nicht vollständig zustimmen, dürfen Sie die Software nicht installieren und/oder verwenden. Sie stimmen als Empfänger einer übertragenen Lizenz weiterhin zu, dass Sie über keine zusätzlichen oder besseren Rechte verfügen, als der ursprüngliche Endnutzer, der die Software vom Rechtsinhaber erworben hat.

2.6 Ab dem Zeitpunkt der Aktivierung der Software bzw. Installation der Lizenzschlüsseldatei (mit Ausnahme einer Testversion der Software) haben Sie das Recht, folgende Dienstleistungen für den auf der Softwareverpackung (falls Sie Software auf einem physischen Medium erworben haben) oder während des Erwerbs (falls die Software über das Internet erworben wurde) festgelegten Zeitraum zu beziehen:

- Updates der Software über das Internet, wenn und wie der Rechtsinhaber diese auf seiner Webseite oder mittels anderer Online-Dienste veröffentlicht. Jedwede Updates, die Sie erhalten, werden Teil der Software und die Geschäftsbedingungen dieses Vertrags gelten für diese;

- Technische Unterstützung über das Internet sowie technische Unterstützung über die Telefon-Hotline.

3. Aktivierung und Zeitraum

3.1. Falls Sie Modifikationen an Ihrem Computer oder an der darauf installierten Software anderer Anbieter vornehmen, kann der Rechtsinhaber von Ihnen verlangen, die Aktivierung der Software bzw. die Installation der Lizenzschlüsseldatei zu wiederholen. Der Rechtsinhaber behält sich das Recht vor, jegliche Mittel und Verifizierungsverfahren zu nutzen, um die Gültigkeit der Lizenz und/oder die Rechtmäßigkeit einer Kopie der Software, die auf Ihrem Computer installiert und/oder genutzt wird, zu verifizieren.

3.2. Falls die Software auf einem physischen Medium erworben wurde, kann die Software nach Ihrer Annahme dieses Vertrags mit Beginn ab dem Zeitpunkt der Annahme dieses Vertrags für die auf der Verpackung bezeichnete Periode genutzt werden.

3.3. Falls die Software über das Internet erworben wurde, kann die Software nach Ihrer Annahme dieses Vertrags für die während des Erwerbs bezeichnete Zeitdauer genutzt werden.

3.4. Sie haben das Recht, eine Testversion der Software zu nutzen, und zwar gemäß der Festlegung in Klausel 2.1 und ohne jedwede Gebühr für die einzelne geltende Evaluierungsperiode (30 Tage) ab dem Zeitpunkt der Aktivierung der Software im Einklang mit diesem Vertrag, *und zwar unter der Bedingung, dass* die Testversion Ihnen nicht das Recht auf Updates und technische Unterstützung über das Internet und technische Unterstützung über die Telefon-Hotline einräumt. Wenn der Rechtsinhaber für die einzelne geltende Evaluierungsperiode einen anderen Zeitraum festlegt, erhalten Sie darüber eine Mitteilung.

3.5. Ihre Lizenz zur Nutzung der Software beschränkt sich auf den in den Klauseln 3.2 oder 3.3 (je nach Anwendbarkeit) bezeichneten Zeitraum. Die verbleibende Zeitdauer kann auf die im Benutzerhandbuch beschriebene Weise abgefragt werden.

3.6. Haben Sie die Software zur Nutzung auf mehr als einem Computer erworben, beginnt der Zeitraum, auf den Ihre Lizenz zur Nutzung der Software begrenzt ist, am Tag der Aktivierung der Software bzw. der Installation der Lizenzschlüsseldatei auf dem ersten Computer.

3.7. Unbeschadet anderer Rechtsmittel laut Gesetz oder Billigkeitsrecht, zu denen der Rechtsinhaber im Falle eines Verstoßes gegen die Geschäftsbedingungen dieses Vertrags durch Sie berechtigt ist, ist der Rechtsinhaber jederzeit, ohne Sie benachrichtigen zu müssen, dazu berechtigt, diese Lizenz zur Nutzung der Software zu kündigen, und zwar ohne den Verkaufspreis oder einen Teil davon zurückzuerstatten.

3.8. Sie stimmen zu, dass Sie bei der Nutzung der Software sowie bei der Verwendung jedweder Berichte oder Informationen, die sich als Ergebnis der Nutzung der Software ableiten, alle geltenden internationalen, nationalen, staatlichen, regionalen und lokalen Gesetze sowie gesetzlichen Bestimmungen, einschließlich (und ohne Beschränkung) Datenschutz-, Urheber-, Exportkontroll- und Verfassungsrecht, einhalten werden.

3.9. Außer wenn anderweitig hierin festgelegt, dürfen Sie keines der Rechte, die Ihnen unter diesem Vertrag gewährt werden, bzw. keine Ihrer hieraus entstehenden Pflichten übertragen oder abtreten.

3.10. Der Rechtsinhaber behält sich das Recht vor, die Möglichkeit zur Aktivierung der Software außerhalb der Region, in der sie vom Rechtsinhaber und/oder seinen Partnern erworben wurde, zu beschränken.

3.11. Wenn Sie die Software mit einem Aktivierungscode erworben haben, der gültig für eine Sprachversion der Software in der Region ist, in der sie vom Rechtsinhaber oder seinen Partnern erworben wurde, dann können Sie die Software nicht durch Anwendung eines Aktivierungscodes aktivieren, der für eine andere Sprachversion vorgesehen ist.

3.12. Im Falle von Beschränkungen, die unter den Punkten 3.10 und 3.11 spezifiziert werden, wird die entsprechende Information über diese Beschränkungen auf der Verpackung und/oder Internetseite des Rechtsinhabers und/oder seiner Partner angegeben.

4. Technische Unterstützung

4.1. Die in Klausel 2.6 dieses Vertrags erläuterte technische Unterstützung wird Ihnen gewährt, wenn das neueste Update der Software installiert wird (außer im Fall einer Testversion der Software).

Technischer Support: http://support.kaspersky.de

5. Sammeln von Informationen

5.1. Durch Zustimmung zu den Geschäftsbedingungen dieses Vertrags haben Sie eingewilligt, dem Rechtsinhaber Informationen über die ausführbaren Dateien und ihre Prüfsummen zur Verfügung zu stellen, um Ihr Sicherheits-Schutzniveau zu verbessern.

5.2. Um das Sicherheitsbewusstsein bezüglich neuer Bedrohungen und deren Quellen zu verbessern, bzw. um Ihr Sicherheits-Schutzniveau zu verbessern, ist der Rechtsinhaber ausdrücklich berechtigt, mit Ihrer Zustimmung, die ausdrücklich in der Kaspersky Security Network Datenerfassungserklärung bestätigt wurde, derartige Informationen zu empfangen. Sie können den Kaspersky Security Network Service während der Installation deaktivieren. Sie können ebenfalls jederzeit auf der Softwareoptionsseite den Kaspersky Security Network Service aktivieren und deaktivieren.

Sie bestätigen und erkennen weiterhin an, dass jedwede Informationen, die vom Rechtsinhaber erfasst werden, zum Zweck der Verfolgung und Veröffentlichung von Sicherheitsrisikotrends verwendet werden können, und zwar nach freiem Ermessen des Rechtsinhabers.

5.3. Die Software verarbeitet keine personenbezogenen Daten und kombiniert keine Verarbeitungsdaten und persönlichen Informationen.

5.4. Sollten Sie nicht wünschen, dass die von der Software gesammelten Informationen an den Rechtsinhaber geschickt werden, sollten Sie den Kaspersky Security Network Service nicht aktivieren und/oder deaktivieren.

6. Beschränkungen

6.1. Sie werden die Software nicht emulieren, klonen, vermieten, verleihen, leasen, verkaufen, modifizieren, dekompilieren oder zurückentwickeln oder disassemblieren oder Arbeiten auf Grundlage der Software oder eines Teils davon ableiten, jedoch mit der einzigen Ausnahme eines Ihnen durch geltende Gesetzgebung gewährten Rechts, von dem keine Rücktretung möglich ist, und Sie werden in keiner anderen Form irgendeinen Teil der Software in menschlich lesbare Form umwandeln oder die lizenzierte Software oder irgendeine Teilmenge der lizenzierten Software übertragen, noch irgendeiner Drittpartei gestatten, dies zu tun, außer im Umfang vorangegangener Einschränkungen, die ausdrücklich durch geltendes Recht untersagt sind. Weder Binärcode noch Quellcode der Software dürfen verwendet oder zurückentwickelt werden, um den Programmalgorithmus, der proprietär ist, wiederherzustellen. Alle Rechte, die nicht ausdrücklich hierin gewährt werden, verbleiben beim Rechtsinhaber und/oder dessen Zulieferern, je nachdem, was zutrifft. Jegliche derartige nicht autorisierte Nutzung der Software kann zur sofortigen und automatischen Kündigung dieses Vertrags sowie der hierunter gewährten Lizenz und zu Ihrer straf- und/oder zivilrechtlichen Verfolgung führen.

6.2. Sie werden die Rechte zur Nutzung der Software nicht an eine Drittpartei übertragen, außer entsprechend der Festlegung in Klausel 2.5 dieses Vertrags.

6.3. Sie werden den Aktivierungscode und/oder die Lizenzschlüssel-Datei keinen Drittparteien verfügbar machen oder Drittparteien Zugang zum Aktivierungscode und/oder zum Lizenzschlüssel gewähren. Aktivierungscode und/oder Lizenzschlüssel werden/wird als vertrauliche Daten des Rechtsinhabers betrachtet, und Sie werden angemessene Sorgfalt zum Schutz der Vertraulichkeit des Aktivierungscodes und/oder des Lizenzschlüssels walten lassen, sofern Sie den Aktivierungscode und/oder den Lizenzschlüssel entsprechend der Festlegung in Klausel 2.5 dieses Vertrags an Drittparteien übertragen dürfen.

6.4. Sie werden die Software nicht an eine Drittpartei vermieten, verleasen oder verleihen.

6.5. Sie werden die Software nicht zur Erstellung von Daten oder Software verwenden, die zur Feststellung, zum Sperren oder zur Handhabung von Bedrohungen, wie im Nutzerhandbuch beschrieben, genutzt werden.

6.6. Der Rechtsinhaber hat das Recht, die Schlüsseldatei zu blockieren oder Ihre Lizenz zu kündigen, falls Sie gegen irgendwelche Geschäftsbedingungen dieses Vertrags verstoßen, und zwar ohne irgendeine Rückerstattung an Sie.

6.7. Falls Sie die Testversion der Software verwenden, sind Sie nicht berechtigt, technische Unterstützung, wie in Klausel 4 dieses Vertrags festgelegt, zu erhalten, und Sie sind ebenfalls nicht berechtigt, die Lizenz oder die Rechte zur Nutzung der Software an irgendeine Drittpartei zu übertragen.

7. Eingeschränkte Garantie und Haftungsausschluss

7.1. Der Rechtsinhaber garantiert, dass die Software im Wesentlichen im Einklang mit den im Nutzerhandbuch dargelegten Spezifikationen und Beschreibungen funktionieren wird, *jedoch vorausgesetzt,* dass eine solche eingeschränkte Garantie nicht für Folgendes gilt: (w) Mängel Ihres Computers und zugehörigen Verstoß, wofür der Rechtsinhaber ausdrücklich jedwede Gewährleistungsverantwortung ablehnt; (x) Funktionsstörungen, Defekte oder Ausfälle, resultierend aus falscher Verwendung, Missbrauch, Unfall, Nachlässigkeit, unsachgemäßer/m Installation, Betrieb oder Wartung, Diebstahl, Vandalismus, höherer Gewalt, terroristischen Akten, Stromausfällen oder -schwankungen, Unglück, Veränderung, nicht zulässiger Modifikation oder Reparaturen durch eine Partei außer dem Rechtsinhaber oder Maßnahmen einer sonstigen Drittpartei oder Aktionen ihrerseits, oder Ursachen außerhalb der Kontrolle des Rechtsinhabers; (y) jedweder Defekt, der dem Rechtsinhaber nicht durch Sie bekannt gemacht wird, sobald dies nach dem ersten Auftreten des Defekts möglich ist; und (z) Inkompatibilität, verursacht durch Hardware- und/oder Software-Komponenten, die auf Ihrem Computer installiert sind.

7.2. Sie bestätigen, akzeptieren und erkennen an, dass keine Software frei von Fehlern ist, und Sie sind angehalten, den Computer mit einer für Sie geeigneten Häufigkeit und Beständigkeit zu sichern.

7.3. Der Rechtsinhaber gibt keine Garantie, dass die Software im Fall von Verstößen gegen die Bedingungen, wie im Nutzerhandbuch oder in diesem Vertrag beschrieben, einwandfrei funktionieren wird.

7.4. Der Rechtsinhaber garantiert nicht, dass die Software einwandfrei funktionieren wird, wenn Sie nicht regelmäßig, wie in Klausel 2.6 dieses Vertrags erläutert, Updates herunterladen.

7.5. Der Rechtsinhaber garantiert keinen Schutz vor im Nutzerhandbuch beschriebenen Bedrohungen nach Ablauf der in Klausel 3.2 oder 3.3 dieses Vertrags bezeichneten Periode oder nachdem die Lizenz zur Nutzung der Software aus irgendeinem Grund gekündigt wurde.

7.6. DIE SOFTWARE WIRD OHNE MÄNGELGEWÄHR BEREITGESTELLT UND DER RECHTSINHABER GIBT KEINE ZUSICHERUNG UND KEINE GEWÄHRLEISTUNG IN BEZUG AUF IHRE NUTZUNG ODER LEISTUNG. DER RECHTSINHABER UND SEINE PARTNER GEWÄHREN AUßER DEN GARANTIEN, ZUSICHERUNGEN, BESTIMMUNGEN ODER BEDINGUNGEN, DIE DURCH GELTENDES RECHT NICHT AUSGESCHLOSSEN ODER BESCHRÄNKT WERDEN KÖNNEN, KEINE GARANTIEN, ZUSICHERUNGEN, BESTIMMUNGEN ODER BEDINGUNGEN (AUSDRÜCKLICHER ODER STILLSCHWEIGENDER NATUR, DIE ENTWEDER AUS EINER GESCHÄFTSBEZIEHUNG ODER EINEM HANDELSBRAUCH ENTSTEHEN BZW. AUS GESETZLICHEN, GEWOHNHEITSRECHTLICHTEN ODER ANDEREN VORSCHRIFTEN ABGELEITET WERDEN) HINSICHTLICH JEDWEDER ANGELEGENHEIT, EINSCHLIEßLICH (OHNE EINSCHRÄNKUNG) VON NICHTVERLETZUNG VON RECHTEN DRITTER, MARKTGÄNGIGKEIT, BEFRIEDIGENDE QUALITÄT, INTEGRIERUNG ODER BRAUCHBARKEIT FÜR EINEN BESTIMMTEN ZWECK. SIE TRAGEN DAS GESAMTE STÖRUNGSRISIKO UND DAS GESAMTRISIKO HINSICHTLICH DER LEISTUNG UND VERANTWORTUNG FÜR DIE AUSWAHL DER SOFTWARE, UM IHRE VORGESEHENEN RESULTATE ZU ERZIELEN, UND FÜR DIE INSTALLATION SOWIE DIE NUTZUNG DER SOFTWARE UND DIE MIT IHR ERZIELTEN ERGEBNISSE. OHNE EINSCHRÄNKUNG DER VORANGEGANGENEN BESTIMMUNGEN MACHT DER RECHTSINHABER KEINE ZUSICHERUNGEN UND GIBT KEINE GEWÄHRLEISTUNG, DASS DIE SOFTWARE FEHLERFREI ODER FREI VON UNTERBRECHUNGEN ODER SONSTIGEN STÖRUNGEN IST ODER DASS DIE SOFTWARE JEDWEDE ODER ALL IHRE ANFORDERUNGEN ERFÜLLEN WIRD, UNGEACHTET DESSEN, OB GEGENÜBER DEM RECHTSINHABER OFFEN GELEGT ODER NICHT.

8. Haftungsausschluss und Haftungsbeschränkungen

8.1. INSOWEIT GESETZLICH STATTHAFT, SIND DER RECHTSINHABER UND SEINE PARTNER UNTER KEINEN UMSTÄNDEN HAFTBAR FÜR JEDWEDE SPEZIELLEN ODER BEILÄUFIGEN SCHÄDEN, STRAFZUSCHLAG ZUM SCHADENERSATZ, INDIREKTE ODER FOLGESCHÄDEN (EINSCHLIEßLICH UND NICHT BESCHRÄNKT AUF SCHÄDEN AUS VERLUST VON GEWINN ODER VERTRAULICHEN ODER SONSTIGEN INFORMATIONEN, FÜR GESCHÄFTSUNTERBRECHUNG, FÜR VERLUST VON PRIVATSPHÄRE, KORRUPTION, BESCHÄDIGUNG UND VERLUST VON DATEN ODER PROGRAMMEN, FÜR VERSÄUMNIS EINER PFLICHTERFÜLLUNG, EINSCHLIEßLICH JEDWEDER GESETZLICHER PFLICHTEN, TREUEPFLICHT ODER PFLICHT ZUR WAHRUNG ANGEMESSENER SORGFALT, FÜR NACHLÄSSIGKEIT, FÜR WIRTSCHAFTLICHEN VERLUST UND FÜR FINANZIELLEN ODER JEDWEDEN SONSTIGEN VERLUST), DIE AUS ODER AUF IRGENDEINE WEISE IM ZUSAMMENHANG MIT DER NUTZUNG ODER UNMÖGLICHKEIT DER NUTZUNG DER SOFTWARE, DER BEREITSTELLUNG ODER DEM VERSÄUMNIS DER BEREITSTELLUNG TECHNISCHER UNTERSTÜTZUNG ODER SONSTIGER DIENSTLEISTUNGEN, INFORMATIONEN, SOFTWARE UND ZUGEHÖRIGEM INHALT MITTELS DER SOFTWARE RESULTIEREN, ODER SICH ANDERWEITIG AUS DER NUTZUNG DER SOFTWARE ODER ANDERWEITIG UNTER BZW. IM ZUSAMMENHANG MIT EINER BESTIMMUNG DIESES VERTRAGS ERGEBEN, ODER DIE FOLGE EINES VERTRAGSBRUCHS ODER UNERLAUBTER HANDLUNG (EINSCHLIEßLICH NACHLÄSSIGKEIT, FALSCHANGABE, JEDWEDER STRIKTEN HAFTUNGSVERPFLICHTUNG ODER -PFLICHT), ODER EINER VERLETZUNG GESETZLICHER PFLICHTEN ODER DER GEWÄHRLEISTUNG DES RECHTSINHABERS ODER EINES SEINER PARTNER SIND, UND ZWAR AUCH DANN NICHT, WENN DER RECHTSINHABER ODER EINER SEINER PARTNER BEZÜGLICH DER MÖGLICHKEIT SOLCHER SCHÄDEN INFORMIERT WURDE.

SIE STIMMEN ZU, DASS IN DEM FALL, DASS DER RECHTSINHABER UND/ODER SEINE PARTNER HAFTBAR GEMACHT WERDEN/WIRD, DIE HAFTUNG DES RECHTSINHABERS UND/ODER SEINER PARTNER AUF DIE KOSTEN DER SOFTWARE BESCHRÄNKT IST. UNTER KEINEN UMSTÄNDEN WIRD DIE HAFTUNG DES RECHTSINHABERS UND/ODER SEINER PARTNER DIE FÜR DIE SOFTWARE ERSTATTETEN KOSTEN AN DEN RECHTSINHABER ODER DEN PARTNER ÜBERSTEIGEN (JE NACHDEM, WAS ZUTRIFFT).

NICHTS IN DIESEM VERTRAG SCHLIEßT EINEN ANSPRUCH AUFGRUND VON TOD UND PERSONENSCHADEN AUS ODER SCHRÄNKT DIESEN EIN. IN DEM FALL, DASS EIN HAFTUNGSAUSSCHLUSS, EIN AUSSCHLUSS

ODER EINE EINSCHRÄNKUNG IN DIESEM VERTRAG AUFGRUND GELTENDEN RECHTS NICHT AUSGESCHLOSSEN ODER BESCHRÄNKT WERDEN KANN, WIRD NUR EIN SOLCHER HAFTUNGSAUSSCHLUSS, AUSSCHLUSS ODER EINE EINSCHRÄNKUNG NICHT FÜR SIE GELTEN, UND SIE SIND WEITERHIN AN JEDWEDE VERBLEIBENDEN HAFTUNGSAUSSCHLÜSSE, AUSSCHLÜSSE ODER EINSCHRÄNKUNGEN GEBUNDEN.

9. GNU und sonstige Drittpartei-Lizenzen

9.1. Die Software kann einige Softwareprogramme enthalten, die an den Nutzer unter der GPL (GNU General Public License) oder sonstigen vergleichbaren freien Softwarelizenzen lizenziert (oder unterlizenziert) sind und dem Nutzer neben anderen Rechten gestatten, bestimmte Programme oder Teile dieser Programme zu kopieren, zu modifizieren und weiter zu verbreiten und sich Zugang zum Quellcode zu verschaffen („Open Source Software“). Falls es solche Lizenzen erforderlich machen, dass für jedwede Software, die an jemanden in ausführbarem Binärformat geliefert wird, diesen Nutzern der Quellcode ebenfalls verfügbar gemacht wird, dann soll der Quellcode zur Verfügung gestellt werden, indem ein diesbezügliches Ersuchen an source@kaspersky.com gesendet wird, oder der Quellcode wird mit der Software geliefert. Falls irgendwelche Open Source Software-Lizenzen es erforderlich machen, dass der Rechtsinhaber Rechte zur Nutzung, zum Kopieren oder zur Änderung eines Open Source Software-Programms bereitstellt, welche umfassender sind, als die in diesem Vertrag gewährten Rechte, dann werden derartige Rechte Vorrang vor den hierin festgelegten Rechten und Einschränkungen haben.

10. Geistiges Eigentum

10.1. Sie stimmen zu, dass die Software sowie die Urheberschaft, Systeme, Ideen, Betriebsmethoden, Dokumentation und sonstige in der Software enthaltenen Informationen proprietäres geistiges Eigentum und/oder die wertvollen Geschäftsgeheimnisse des Rechtsinhabers oder seiner Partner sind und dass der Rechtsinhaber und seine Partner, je nachdem was zutrifft, durch das Zivil- und Strafrecht sowie durch Gesetze zum Urheberrecht, bezüglich Geschäftsgeheimnissen, Handelsmarken und Patenten der Russischen Föderation, der Europäischen Union und der Vereinigten Staaten sowie anderer Länder und internationaler Übereinkommen geschützt sind. Dieser Vertrag gewährt Ihnen keinerlei Rechte am geistigen Eigentum, einschließlich an jeglichen Handelsmarken und Servicemarken des Rechtsinhabers und/oder seiner Partner („Handelsmarken“). Sie dürfen die Handelsmarken nur so weit nutzen, um von der Software im Einklang mit der akzeptierten Handelsmarkenpraxis erstellte Druckausgaben zu identifizieren, einschließlich der Identifizierung des Namens des Besitzers der Handelsmarke. Eine solche Nutzung der Handelsmarke gibt Ihnen keinerlei Besitzrechte an dieser Handelsmarke. Der Rechtsinhaber und/oder seine Partner besitzen und behalten alle Rechte, Titel und Anteile an der Software, einschließlich (ohne jedwede Einschränkung) jedweden Fehlerkorrekturen, Erweiterungen, Updates oder sonstigen Modifikationen an der Software, ob durch den Rechtsinhaber oder eine beliebige Drittpartei vorgenommen, und allen Urheberrechten, Patenten, Rechten an Geschäftsgeheimnissen, Handelsmarken und sonstigem geistigen Eigentum daran. Ihr Besitz, die Installation oder Nutzung der Software lässt den Titel am geistigen Eigentum an der Software nicht auf Sie übergehen, und Sie erwerben keinerlei Rechte an der Software, außer jene ausdrücklich in diesem Vertrag dargelegten. Alle hierunter erstellten Kopien der Software müssen dieselben proprietären Informationen enthalten, die auf und in der Software erscheinen. Mit Ausnahme der hierin aufgeführten Bestimmungen gewährt Ihnen dieser Vertrag keine Rechte geistigen Eigentums an der Software und Sie bestätigen, dass diese unter diesem Vertrag gewährte Lizenz Ihnen gemäß den weiteren Festlegungen hierin ausschließlich das Recht auf eingeschränkte Nutzung unter den Geschäftsbedingungen dieses Vertrags gewährt. Der Rechtsinhaber behält sich alle Rechte vor, die Ihnen nicht ausdrücklich in diesem Vertrag gewährt wurden.

10.2. Sie stimmen zu, die Software in keinster Weise zu modifizieren oder abzuändern. Sie dürfen die Urheberrechtshinweise oder sonstige proprietäre Hinweise auf jedweden Kopien der Software nicht entfernen oder verändern.

11. Geltendes Recht; Schiedsverfahren

11.1. Dieser Vertrag unterliegt den Gesetzen der Russischen Föderation und wird nach diesen ausgelegt, und zwar ohne Bezug auf gegenteilige gesetzliche Regelungen und Prinzipien. Dieser Vertrag wird nicht dem Übereinkommen der Vereinten Nationen über Verträge über den internationalen Warenverkauf unterliegen, dessen Anwendung ausschließlich ausgeschlossen wird. Jede Meinungsverschiedenheit, die aus den Bedingungen dieses Vertrags, deren Auslegung oder Anwendung oder einem Verstoß gegen diese resultiert, wird, außer falls durch unmittelbare Verhandlung beigelegt, durch das Gericht der internationalen Handelsschiedsgerichtsbarkeit bei der Industrie- und Handelskammer der Russischen Föderation in Moskau, in der Russischen Föderation, beigelegt. Jeder vom Schlichter abgegebene Schiedsspruch ist für die beteiligten Parteien endgültig und bindend und jedwedes Urteil bezüglich eines solchen Schiedsspruchs kann von jedem Gericht der zuständigen Jurisdiktion durchgesetzt werden. Nichts in diesem

Abschnitt 11 wird eine Partei daran hindern, von einem Gericht der zuständigen Jurisdiktion rechtmäßige Entschädigung zu verlangen oder zu erhalten, sei es vor, während oder nach einem Schiedsverfahren.

12. Zeitraum für Rechtsverfolgung

12.1. Von den Parteien dieses Vertrags kann keine Rechtsverfolgung, ungeachtet der Form, die sich aus Transaktionen unter diesem Vertrag ergibt, nach mehr als einem (1) Jahr nach dem Eintreten des Klagegrundes oder der Entdeckung dessen Eintritts ergriffen werden, außer, dass eine Rechtsverfolgung für Verletzung von Rechten geistigen Eigentums innerhalb des maximal geltenden gesetzlichen Zeitraums ergriffen wird.

13. Vollständigkeit der Vereinbarung, Salvatorische Klausel, kein Verzicht

13.1. Dieser Vertrag stellt die Gesamtvereinbarung zwischen Ihnen und dem Rechtsinhaber dar und ersetzt jegliche sonstigen, vorherigen Vereinbarungen, Vorschläge, Kommunikation oder Ankündigung, ob mündlich oder schriftlich, in Bezug auf die Software oder den Gegenstand dieser Vereinbarung. Sie bestätigen, dass Sie diesen Vertrag gelesen haben, ihn verstehen und seinen Bedingungen zustimmen. Falls eine Bestimmung dieses Vertrags von einem Gericht der zuständigen Jurisdiktion insgesamt oder in Teilen als untauglich, ungültig oder aus welchen Gründen auch immer als nicht durchsetzbar angesehen wird, wird diese Bestimmung enger ausgelegt, damit sie rechtmäßig und durchsetzbar wird, und der Gesamtvertrag wird an diesem Umstand nicht scheitern, und die Ausgewogenheit des Vertrags bleibt weiterhin vollinhaltlich gültig und wirksam, so weit gesetzlich oder nach Billigkeitsrecht zulässig, während der ursprüngliche Inhalt weitest möglich beibehalten wird. Kein Verzicht auf eine hierin enthaltene Bestimmung oder Kondition ist gültig, außer in schriftlicher Form und durch Sie und einen autorisierten Vertreter des Rechtsinhabers unterzeichnet, vorausgesetzt, dass kein Verzicht einer Verletzung einer Bestimmung dieses Vertrags einen Verzicht eines vorherigen, gleichzeitigen oder Folgeverstoßes konstituiert. Nichtverfolgung oder fehlende Durchsetzung einer Bestimmung dieses Vertrags durch den Rechtsinhaber kann nicht als Verzicht auf diese Bestimmung oder dieses Recht geltend gemacht werden.

14. Kontaktinformationen des Rechtsinhabers

Sollten Sie Fragen in Bezug auf diesen Vertrag haben oder sollten Sie wünschen, sich aus irgendeinem Grund mit dem Rechtsinhaber in Verbindung zu setzen, kontaktieren Sie bitte unsere Kundendienstabteilung unter:

Kaspersky Lab ZAO, 10 build. 1, 1st Volokolamsky Proezd
Moskau, 123060
Russische Föderation

Tel.: +7-495-797-8700
Fax: +7-495-645-7939

E-Mail: info@kaspersky.com

Webseite: http://www.kaspersky.com

© 1997-2010 Kaspersky Lab ZAO. Alle Rechte vorbehalten. Die Software und jedwede begleitende Dokumentation unterliegen dem Urheberrecht bzw. dem Schutz durch Urheberrechtsgesetze und internationale Urheberrechtsabkommen sowie durch weitere Gesetze und Abkommen zum geistigen Eigentum.

INHALT

LIZENZVEREINBARUNG 3

ÜBER DIESES HANDBUCH 14

In diesem Dokument 14

Formatierung mit besonderer Bedeutung 16

ZUSÄTZLICHE INFORMATIONSQUELLEN 17

KASPERSKY ANTI-VIRUS 2011 19

Lieferumfang 20

Hard- und Softwarevoraussetzungen 20

PROGRAMM INSTALLIEREN 21

Vorbereitung der Installation des Programms 21

Installation des Programms 21

Standardinstallation von Kaspersky Anti-Virus 22

Benutzerdefinierte Installation von Kaspersky Anti-Virus 23

Vorbereitung zur Nutzung des Programms 25

Programm deinstallieren 25

LIZENZVERWALTUNG 26

Über die Lizenz 26

Lizenz-Info anzeigen 27

Lizenz erwerben 27

Lizenz verlängern 28

Über den Lizenzvertrag 29

Über den Aktivierungscode 29

Über den Lizenzschlüssel 29

Kaspersky Anti-Virus aktivieren 29

Testversion aktivieren 30

Programm mithilfe des Aktivierungscodes aktivieren 30

Programm mithilfe der Schlüsseldatei aktivieren 31

PROGRAMMOBERFLÄCHE 32

Symbol von Kaspersky Anti-Virus 32

Programmhauptfenster 34

Programmkonfigurationsfenster 35

Meldungsfenster und Pop-up-Meldungen 36

Benachrichtigungen 37

Benachrichtigungsmethoden 37

Benachrichtigungen konfigurieren 38

Über Pop-up-Meldungen 39

Oberfläche von Kaspersky Anti-Virus anpassen 39

PROGRAMM STARTEN UND BEENDEN 41

Kaspersky Anti-Virus beenden 41

Autostart von Kaspersky Anti-Virus anpassen 41

Energiesparmodus anpassen 42

SCHUTZSTATUS DES COMPUTERS 44
Schutzstatus des Computers einschätzen 44
Sicherheitsassistent 45
LÖSUNGEN FÜR TYPISCHE AUFGABEN 46
Wie eine vollständige Virenuntersuchung des Computers ausgeführt wird 46
Computer schnell untersuchen 47
Dateien, Ordner und Laufwerke auf Viren untersuchen 47
Wie man eine Suche des Computers nach Zeitplan anpasst 47
Wie eine Lizenz erworben und verlängert wird 48
Wie man die Datenbanken und Programm-Module aktualisiert 48
Wie Programmeinstellungen von Kaspersky Anti-Virus auf einen anderen Computer übertragen werden 49
Empfohlene Aktionen bei blockiertem Zugriff auf eine Datei 49
Was tun, wenn Sie vermuten, dass ein Objekt von einem Virus infiziert ist? 50
Wie ein Objekt wiederhergestellt wird, das vom Programm gelöscht oder desinfiziert wurde 51
Wie man in einen Bericht über die Programmarbeit einsieht 51
Was tun, wenn das Programm Meldungen anzeigt? 51
ERWEITERTE PROGRAMMEINSTELLUNGEN 52
Schutzbereich festlegen 52
Zu kontrollierende schädliche Programme auswählen 52
Vertrauenswürdige Zone anlegen 53
Datei-Anti-Virus 56
Deaktivierung des Dateischutzes 57
Computerschutz fortsetzen 59
Datei-Anti-Virus konfigurieren 60
Sicherheitsstufe auswählen 60
Typen der zu untersuchenden Dateien festlegen 61
Schutzbereich festlegen 62
Zusätzliche Parameter anpassen 64
Aktion für Objekte auswählen 65
Standardparameter für den Dateischutz wiederherstellen 66
Statistik über den Dateischutz 66
Virensuche 68
Aufgabenverwaltung Virensuche 68
Untersuchungsaufgaben starten / beenden 69
Untersuchungsaufgaben erstellen 70
Liste der Untersuchungsobjekte erstellen 72
Untersuchungsaufgaben anpassen 74
Sicherheitsstufe auswählen 74
Typen der zu untersuchenden Objekte festlegen 76
Aktion für Objekte auswählen 77
Start der Aufgaben zur Virensuche nach Zeitplan anpassen 78
Untersuchungsaufgaben unter Benutzernamen starten 78
Einheitliche Untersuchungsparameter für alle Aufgaben zur Virensuche festlegen 79
Standardmäßige Untersuchungseinstellungen wiederherstellen 80
Statistik über die Virensuche 81
Programm-Update 83
Update starten 84
Rollback zum vorherigen Update 85

Update von einer lokalen Quelle 86
Update anpassen 87
Updatemodus und Updateobjekt auswählen 88
Updatequelle auswählen 89
Start der Updateaufgaben nach Zeitplan anpassen 90
Einstellungen für Verbindung mit Proxy-Server 91
Statistik für das Update 91
Berichte und Speicher 93
Quarantäne 93
Den Inhalt der Quarantäne anzeigen 93
Objekte in der Quarantäne 94
Quarantäneobjekte nach dem Programmupdate untersuchen 95
Backup 96
Den Inhalt des Backups anzeigen 96
Sicherungskopien verwenden 97
Berichte 98
Berichte und Backups anpassen 100
Berichtsparameter anpassen 100
Einstellungen für Quarantäne und Backup anpassen 101
Teilnahme am Kaspersky Security Network 102
BEDIENUNG DES PROGRAMMS ÜBER DIE BEFEHLSZEILE 104
Hilfe anzeigen 105
Virensuche 105
Programm-Update 107
Rollback zum vorherigen Update 108
Beenden einer Komponente oder einer Aufgabe 109
Statistik über die Arbeit einer Komponente oder Aufgabe 110
Schutzparameter exportieren 110
Schutzparameter importieren 110
Programm aktivieren 111
Programm beenden 111
Rückgabecodes der Befehlszeile 111
KONTAKTAUFNAHME MIT DEM TECHNISCHEN SUPPORT 113
ANHÄNGE 115
Liste der Objekte, die auf ihre Erweiterung untersucht werden 115
Zulässige Ausschlussmasken für Dateien 117
Zulässige Ausschlussmasken gemäß der Klassifikation der Viren-Enzyklopädie 118
GLOSSAR 119
KASPERSKY LAB 123
INFORMATIONEN ZUM FREMDCODE 124
Programmcode 124
ADOBE ABI-SAFE CONTAINERS 1.0 125
BOOST 1.39.0 125
CURL 7.19.3 125
EXPAT 1.2 125
FMT.H 126

GROWL 1.1.5 126
INFO-ZIP 5.51 127
LIBPNG 1.2.8 127
LIBUTF 127
LZMALIB 4.43 128
MD5.H 128
MD5.H 128
RFC1321-BASED (RSA-FREE) MD5 LIBRARY 128
SHA1.C 1.2 128
STLPORT 5.2.1 129
TINYXML 2.5.3 129
WEB-SOCKET-JS 129
ZLIB 1.0.8, 1.2.3 130
Erarbeitungsmittel 130
GCC 4.0.1 130
Andere Informationen 134
SACHREGISTER 135

ÜBER DIESES HANDBUCH

Dieses Dokument ist ein Handbuch zur Installation, Konfiguration und Verwendung des Programms Kaspersky Anti-Virus for Mac 2011. Dieses Dokument richtet sich an ein breites Spektrum von Anwendern. Die Anwender sollten über grundlegende Kenntnisse im Umgang mit Mac-Computern verfügen. Dazu zählen Basiskenntnisse und -Fähigkeiten im Umgang mit dem Betriebssystem Mac OS X und dessen Schnittstelle sowie mit den E-Mail- und Internet-Programmen.

Das Dokument soll:

- dem Anwender helfen, das Programm selbst auf einem Computer zu installieren, es zu aktivieren und unter Berücksichtigung individueller Aufgaben optimal anzupassen.
- es soll eine schnelle Suche von Informationen sicher stellen, die für die Entscheidung von mit dem Programm verbundenen Fragen notwendig ist;
- zusätzliche Informationsquellen zum Programm und Wege zur Kontaktaufnahme mit dem technischen Support von Kaspersky Lab beleuchten.

IN DIESEM ABSCHNITT

In diesem Dokument 14

Formatierung mit besonderer Bedeutung 16

IN DIESEM DOKUMENT

Das Benutzerhandbuch für Kaspersky Anti-Virus 2011 umfasst die folgenden Abschnitte:

Zusätzliche Informationsquellen

Dieser Abschnitt nennt Quellen, die zusätzliche Informationen über das Programm bieten, und verweist auf Internetressourcen, die zur Diskussion über das Programm, für Vorschläge, sowie für Fragen und Antworten dienen.

Kaspersky Anti-Virus 2011

Dieser Abschnitt enthält eine Beschreibung der Möglichkeiten des Programms sowie eine kurze Angabe über ihre Komponenten und Grundfunktionen. Hier können Sie mehr über den Lieferumfang und die Services erfahren, die den registrierten Programmnutzern zur Verfügung stehen. Außerdem werden die Hard- und Softwarevoraussetzungen genannt, denen ein Computer entsprechen muss, damit Kaspersky Anti-Virus darauf installiert werden kann.

Programm installieren

Dieser Abschnitt enthält die Anweisungen, die Ihnen dabei helfen sollen, das Programm lokal auf Ihrem Computer zu installieren. Dieser Abschnitt beschreibt, wie das Programm von einem Computer deinstalliert wird.

Lizenzverwaltung

Dieser Abschnitt informiert über die wichtigsten Begriffe, die mit der Programmlizenzierung zusammenhängen. Hier können Sie erfahren, wie das Programm aktiviert wird und wo Sie die Informationen zur aktuellen Lizenz ansehen können. Außerdem finden Sie hier Informationen darüber, wie Sie eine Lizenz erwerben und ihre Gültigkeitsdauer verlängern können.

Programmoberfläche

Dieser Abschnitt beschreibt die wichtigsten Elemente der grafischen Programmoberfläche: Symbol und Kontextmenü des Programms, Hauptfenster, Konfigurationsfenster und Meldungsfenster.

Programm starten und beenden

Dieser Abschnitt informiert darüber, wie das Programm gestartet und beendet wird.

Schutzstatus des Computers

Dieser Abschnitt informiert darüber, wie ermittelt wird, ob der Computer im Augenblick geschützt ist oder ob seine Sicherheit bedroht ist. Außerdem wird beschrieben, wie man vorhandene Bedrohungen mit Hilfe des Sicherheitsassistenten neutralisiert.

Lösungen für typische Aufgaben

Dieser Abschnitt beschreibt Aufgaben, die sich den meisten Benutzern bei der Arbeit mit dem Programm stellen, und bietet eine Anleitung zur Ausführung dieser Aufgaben.

Erweiterte Programmeinstellungen

Dieser Abschnitt informiert ausführlich über die einzelnen Komponenten und beschreibt den jeweiligen Funktionsalgorithmus und die Einstellungen.

Bedienung des Programms über die Befehlszeile

In diesem Abschnitt wird ausführlich beschrieben, wie das Programm und dessen Komponenten mit der Befehlszeile bedient werden.

Kontaktaufnahme mit dem technischen Support

Dieser Abschnitt enthält Tipps zur Kontaktaufnahme mit dem technischen Support von Kaspersky Lab.

Anhänge

Dieser Abschnitt enthält Hilfeinformationen, die den Haupttext des Dokuments ergänzen.

Glossar

Dieser Abschnitt enthält eine Liste und Definitionen der Begriffe, die in diesem Dokument vorkommen.

FORMATIERUNG MIT BESONDERER BEDEUTUNG

Die Bedeutung der im Handbuch verwendeten Textformatierungen wird in folgender Tabelle erläutert.

Tabelle 1. Formatierung mit besonderer Bedeutung

TEXTBEISPIEL	BESCHREIBUNG DER FORMATIERUNG
Beachten Sie, dass...	Warnungen sind rot geschrieben und eingerahmt. Warnungen enthalten wichtige Informationen, die z.B. auf Aktionen hinweisen, die im Hinblick auf die Computersicherheit als kritisch gelten.
Es wird empfohlen,...	Hinweise sind eingerahmt. Hinweise enthalten hilfreiche und informative Angaben.
Beispiel: ...	Beispiele sind gelb unterlegt und mit "Beispiel" überschrieben.
Ein *Virus* ist...	Neue Begriffe sind kursiv geschrieben.
Command-A	Die Tastenbezeichnungen werden durch Fettdruch hervorgehoben. Die Tastenbezeichnungen, die mit einem Minuszeichen verbunden sind, bedeuten eine Tastenkombination.
Aktivieren	Die Namen von Elementen der Benutzeroberfläche (z.B. Eingabefelder, Menübefehle, Schaltflächen) sind halbfett geschrieben.
➧ *Gehen Sie folgendermaßen vor, um den Aufgabenzeitplan anzupassen:*	Anleitungen sind durch einen Pfeil markiert. Der erste Satz einer Anleitung ist kursiv geschrieben.
`kav update`	Text in der Befehlszeile oder Meldungstext, die das Programm auf dem Bildschirm anzeigt, werden durch eine eigene Schriftart hervorgehoben.
<IP-Adresse Ihres Computers>	Variablen stehen in spitzen Klammern. Eine Variable wird in einem konkreten Fall durch einen entsprechenden Wert ersetzt. Dabei fallen die spitzen Klammern weg.

ZUSÄTZLICHE INFORMATIONSQUELLEN

Bei Fragen über die Anwendung stehen folgende Informationsquellen zur Verfügung:

- Webseite von Kaspersky Lab
- Webseite des technischen Supports (Wissensdatenbank)
- Benutzerforum für Kaspersky-Lab-Produkte
- elektronisches Hilfesystem.

Webseite von Kaspersky Lab

Auf der Internetseite (http://www.kaspersky.com/de/anti-virus_for_mac) finden Sie Angaben über Kaspersky Anti-Virus 2011, die Optionen und Besonderheiten. In unserem Online-Shop können Sie Kaspersky Anti-Virus 2011 erwerben oder die Nutzungsdauer verlängern.

Webseite des technischen Supports (Wissensdatenbank)

Die Wissensdatenbank, die Bestandteil der Webseite des technischen Supports (http://support.kaspersky.com/de/kavmac) ist, bietet Tipps zur Verwendung von Kaspersky-Lab-Produkten. Auf dieser Seite finden Sie Artikel, die von Spezialisten des technischen Supports veröffentlicht wurden.

Diese Artikel bieten nützliche Informationen, Tipps und Antworten auf häufige Fragen zu Kauf, Installation und Verwendung von Kaspersky Anti-Virus 2011. Sie sind nach Themen wie "Problembehebung", "Einstellung von Updates" oder "Einstellung von Datei-Anti-Virus" geordnet. Die Artikel können auch Fragen behandeln, die nicht nur dieses Programm betreffen, sondern auch andere Produkte von Kaspersky Lab. Außerdem können sie allgemeine Neuigkeiten über den Technischen Support beinhalten.

Um die Wissensdatenbank aufzurufen, öffnen Sie das Programmhauptfenster (siehe Seite 34), klicken Sie auf die Schaltfläche und im folgenden Fenster auf die Schaltfläche **Technischer Support**.

Benutzerforum

Wenn Ihre Frage keine dringende Antwort erfordert, können Sie sie mit den Spezialisten von Kaspersky Lab und mit anderen Anwendern in unserem Forum (www.kaspersky.de/forum) diskutieren. Dort sehen Sie Fragen, Kommentare und Vorschläge von Programmbenutzern.

Im Forum können Sie bereits veröffentlichte Themen nachlesen, eigene Kommentare verfassen, neue Themen eröffnen und die Hilfefunktion verwenden.

Um diese Ressource aufzurufen, öffnen Sie das Programmhauptfenster (siehe Seite 34), klicken Sie auf die Schaltfläche und im folgenden Fenster auf die Schaltfläche **Forum**.

Elektronisches Hilfesystem

Das Programm umfasst Dateien mit vollständiger und kontextabhängiger Hilfe . Die Datei mit vollständiger Hilfe enthält Angaben darüber, wie man die Sicherheit des Computers verwaltet: den Schutzzustand einsehen, unterschiedliche Computerbereiche auf Viren prüfen, Updates durchführen, mit Berichten und Quarantänen arbeiten. Außerdem können Sie in der Datei mit der kontextabhängigen Hilfe Angaben über jedes Programmfenster finden: eine Liste und Beschreibung der darin vorgestellten Parameter und eine Liste der zu lösenden Aufgaben.

Um die vollständige Hilfe zu öffnen, öffnen Sie das Programmhauptfenster (siehe Seite 34) und klicken Sie auf die Schaltfläche . Um die Kontexthilfe zu öffnen, klicken Sie im entsprechenden Fenster oder auf einer Registerkarte auf die Schaltfläche .

Wenn Sie in der Wissensdatenbank, im Benutzerforum, im Hilfesystem und in der Dokumentation keine Lösung für Ihr Problem finden können, empfehlen wir Ihnen, sich an den technischen Support von Kaspersky Lab zu wenden (siehe Abschnitt "Kontaktaufnahme mit dem technischen Support" auf Seite 113).

KASPERSKY ANTI-VIRUS 2011

Kaspersky Anti-Virus for Mac 2011 (nachfolgend auch Kaspersky Anti-Virus genannt) ermöglicht den Schutz der Computer mit dem Betriebssystem Mac OS X vor Viren und schädlichen Programmen. Die Anwendung verfügt über folgende Funktionen:

Datei-Anti-Virus

Echtzeitschutz für das Dateisystem des Computers: Zugriffe auf das Dateisystem werden abgefangen und analysiert, schädliche Objekte werden gelöscht, möglicherweise infizierte Objekte werden isoliert, um später analysiert zu werden.

Virensuche

Manuelle Suche und Neutralisierung des schädlichen Codes auf Anfrage des Benutzers: Suche und Analyse von infizierten und möglicherweise infizierten Objekten in festgelegten Untersuchungsbereichen, Objekte werden desinfiziert, gelöscht oder für eine weitere Analyse isoliert.

Im Lieferumfang von Kaspersky Anti-Virus sind folgende Untersuchungsaufgaben enthalten: vollständige Untersuchung aller Objekte des Computers und schnelle Untersuchung von kritischen Bereichen.

Update

Die Datenbanken und Module von Kaspersky Anti-Virus werden von den Kaspersky-Lab-Updateservern aktualisiert. Es werden Sicherungskopien aller zu aktualisierenden Dateien angelegt, um das letzte Update bei Bedarf rückgängig zu machen (Rollback). Heruntergeladene Updates können in eine lokale Quelle kopiert werden, die anderen Netzwerkcomputern als Updatequelle dienen kann, um Datenverkehr einzusparen (Update-Verteilung).

Quarantäne

Verschieben von möglicherweise infizierten Objekten in die Quarantäne: Möglicherweise infizierte Objekte werden in einem Quarantäneordner gespeichert. Sie können später mit aktualisierten Datenbanken untersucht oder vom Benutzer manuell aus der Quarantäne wiederhergestellt werden.

Backup

Vor dem Desinfizieren oder Löschen eines Objekts wird im Backup eine Sicherungskopie davon angelegt. Dadurch besteht die Möglichkeit, das Objekt wiederherzustellen, um darin enthaltene Informationen zu retten.

Berichte

Erstellen eines ausführlichen Berichts über die Arbeit der einzelnen Komponenten von Kaspersky Anti-Virus.

Benachrichtigungen

Benachrichtigung des Benutzers beim Eintreten bestimmter Ereignisse: Sie können für jeden Ereignistyp eine Benachrichtigungsmethode wählen: Tonsignal oder Pop-up-Meldung.

Sie können das Aussehen von Kaspersky Anti-Virus anpassen, indem Sie eigene grafische Elemente und Farbschemata verwenden.

Bei der Arbeit mit Kaspersky Anti-Virus werden Sie umfassend mit Informationen unterstützt: die Anwendung zeigt Meldungen über den Schutzstatus an und verfügt über ein umfassendes Hilfesystem. Der im Lieferumfang der Anwendung enthaltene Sicherheitsassistent (auf Seite 45) vermittelt Ihnen ein vollständiges Bild des aktuellen Schutzzustands Ihres Computers und ermöglicht das umgehende Beheben vorhandener Probleme.

IN DIESEM ABSCHNITT

Lieferumfang 20

Hard- und Softwarevoraussetzungen 20

LIEFERUMFANG

Kaspersky Anti-Virus können Sie bei unseren Vertriebspartnern (Box-Variante) sowie in einem Online-Shop (zum Beispiel auf www.kaspersky.com/de/store unter **Online-Shop**) erwerben.

Wurde das Programm in einer CD-Box erworben, gehören zum Lieferumfang des Programms:

- Versiegelter Umschlag mit Installations-CD, auf der die Programmdateien und die Dokumentation im PDF-Format gespeichert sind.
- Lizenzvertrag.

Zusätzlich zum Lieferumfang können mit eingeschlossen werden:

- Benutzerhandbuch in gedruckter Form (wenn Position im Auftrag enthalten war) oder Programmführer.
- Schlüsseldatei für die Anwendung (auf einer speziellen Diskette gespeichert).
- Aktivierungseinleger (mit dem Aktivierungscodes des Produkts).

Lesen Sie sich vor dem Öffnen des Umschlags mit der CD die Lizenzvereinbarung sorgfältig durch. Mit dem Öffnen des versiegelten Pakets mit der Installations-CD nehmen Sie die Bedingungen der Lizenzvereinbarung an.

Bei Erwerb von Kaspersky Anti-Virus in einem Online-Shop kopieren Sie die Software zusammen mit diesem Handbuch im PDF-Format von der Kaspersky-Lab-Webseite. Die Schlüsseldatei bzw. der Aktivierungscode wird Ihnen nach Zahlungseingang per E-Mail zugeschickt.

HARD- UND SOFTWAREVORAUSSETZUNGEN

Damit Kaspersky Anti-Virus ordnungsgemäß ausgeführt werden kann, muss der Computer die folgenden Mindestanforderungen erfüllen:

- Mac-Computer mit Intel-Prozessor (PowerPC wird nicht unterstützt)
- 512 MB Arbeitsspeicher;
- 270 MB freier Festplattenspeicher (je nach Größe der Antiviren-Datenbanken);
- Betriebssystem Mac OS X 10.5 oder 10.6.

PROGRAMM INSTALLIEREN

Dieser Abschnitt enthält die Anweisungen, die Ihnen dabei helfen sollen, das Programm lokal auf Ihrem Computer zu installieren. Dieser Abschnitt beschreibt, wie das Programm von einem Computer deinstalliert wird.

Zum Lieferumfang von Kaspersky Anti-Virus gehört das Installations- und Deinstallationsprogramm für Kaspersky Anti-Virus.

Es wird empfohlen, vor Installation des neuen Produktes Kaspersky Anti-Virus 2011 for Mac die vorherige Version von Kaspersky Anti-Virus for Mac zu deinstallieren. Verwenden Sie dazu Kaspersky Anti-Virus 2011 Uninstaller (siehe Abschnitt "Programm deinstallieren" auf Seite 25), der zum Lieferumfang des Produktes gehört.

IN DIESEM ABSCHNITT

Vorbereitung der Installation des Programms 21

Installation des Programms 21

Vorbereitung zur Nutzung des Programms 25

Programm deinstallieren 25

VORBEREITUNG DER INSTALLATION DES PROGRAMMS

Vor der Installation von Kaspersky Anti-Virus müssen Sie die folgenden Vorbereitungen treffen:

- Vergewissern Sie sich, dass Ihr Computer die Systemvoraussetzungen erfüllt (s. Abschnitt "Hard- und Softwarevoraussetzungen" auf Seite 20).
- Überprüfen Sie die Verbindung Ihres Computers mit dem Internet. Der Zugriff auf das Internet wird für die Aktivierung des Programms mithilfe eines Aktivierungscodes sowie zum Download von Updates benötigt.
- Deinstallieren Sie sonstige Antivirus-Software von Ihrem Computer, um Systemkonflikte und eine Verringerung der Geschwindigkeit des Betriebssystems zu vermeiden.

INSTALLATION DES PROGRAMMS

Sie können eine der folgenden Methoden zur Installation von Kaspersky Anti-Virus auf Ihrem Computer auswählen:

- Standardinstallation (s. Abschnitt "Standardinstallation von Kaspersky Anti-Virus" auf Seite 22).

  Bei Auswahl dieser Variante wird eine Reihe von Komponenten standardmäßig installiert.

- Benutzerdefinierte Installation (s. Abschnitt "Benutzerdefinierte Installation von Kaspersky Anti-Virus" auf Seite 23):

  Ermöglicht die benutzerdefinierte Installation von Programmkomponenten und wird für erfahrene Benutzer empfohlen.

STANDARDINSTALLATION VON KASPERSKY ANTI-VIRUS

Um die Standardinstallation von Kaspersky Anti-Virus auszuführen, gehen Sie folgendermaßen vor:

1. Öffnen Sie die mitgelieferten Dateien von Kaspersky Anti-Virus. Legen siedafür die Installations-CD ins Laufwerk.

   Wenn Sie Kaspersky Anti-Virus im Online-Shop gekauft haben, ist auf der Webseite von Kaspersky Lab das Programm im zip-Format zum Download erhältlich. Entpacken Sie es und starten Sie die Datei .dmg, um die mitgelieferten Dateien zu sehen.

2. Starten Sie das Installationsprogramm von Kaspersky Anti-Virus. Öffnen Sie dafür im Fenster mit dem Distributionsinhalt das Installationspaket **Kaspersky Anti-Virus 2011**.

   Bestätigen Sie den Start des Installationsprogramms im Bestätigungsfenster. Befolgen Sie die Schritte des Installationsprogramms, um das Programm zu installieren.

3. Klicken Sie im Fenster **Einführung** auf die Schaltfläche **Fortfahren**.

4. Lesen Sie danach im Fenster **Bitte lesen** die Informationen zu dem zu installierenden Programm durch.

   Vergewissern Sie sich, dass Ihr Computer die angegebenen Systemvoraussetzungen erfüllt. Um die Informationen auszudrucken, klicken Sie auf die Schaltfläche **Drucken**. Um die Daten in einer Textdatei zu sichern, klicken Sie auf die Schaltfläche **Sichern**. Zum Fortsetzen der Installation klicken Sie auf die Schaltfläche **Fortsetzen**.

5. Machen Sie sich im Fenster **Lizenz** mit der Lizenzvereinbarung zur Nutzung von Kaspersky Anti-Virus vertraut, die zwischen Ihnen und Kaspersky Lab ZAO abgeschlossen wird. Der Text der Vereinbarung ist in verschiedenen Sprachen verfügbar. Um die Lizenzvereinbarung auszudrucken, klicken Sie auf die Schaltfläche **Drucken**. Um die Vereinbarung in einer Textdatei zu sichern, klicken Sie auf die Schaltfläche **Sichern**.

   Wenn Sie mit allen Punkten in der Vereinbarung einverstanden sind, klicken Sie auf die Schaltfläche **Fortfahren**. Daraufhin erscheint das Bestätigungsfenster für Ihre Zustimmung zu den Bedingungen der Lizenzvereinbarung. Sie können folgende Aktionen ausführen:

   - Fortsetzen der Installation von Kaspersky Anti-Virus. Klicken Sie dazu auf die Schaltfläche **Akzeptieren**.
   - Zur Lizenzvereinbarung zurückkehren. Klicken Sie dazu auf die Schaltfläche **Lizenz lesen**.
   - Installation des Programms abbrechen. Klicken Sie dazu auf die Schaltfläche **Ablehnen**.

6. Lesen Sie im Fenster **KSN** die Informationen über die Teilnahme an Kaspersky Security Network durch (s. Abschnitt "An Kaspersky Security Network teilnehmen" auf Seite 102). Eine Beteiligung an diesem Programm sieht vor, dass Informationen über auf Ihrem Computer erkannte neue Bedrohungen, über gestartete Programme und über geladene signierte Programme an Kaspersky Lab geschickt werden. Außerdem werden ein einmaliger Identifikator, der Ihrem Exemplar von Kaspersky Anti-Virus zugewiesen wurde, sowie Systeminformationen gesendet. Es wird dabei garantiert, dass keine persönlichen Daten gesendet werden.

   Wenn Sie mit allen Punkten der Bestimmung über die Verwendung von Kaspersky Security Network einverstanden sind, aktivieren Sie das Kontrollkästchen **Ich akzeptiere die Teilnahmebedingungen an KSN**. Zum Fortsetzen der Installation klicken Sie auf die Schaltfläche **Fortsetzen**.

   Sie können jederzeit Ihre Teilnahme an Kaspersky Security Network verweigern (s. Abschnitt "An Kaspersky Security Network teilnehmen" auf Seite 102).

7. Lesen Sie im Fenster **Installationstyp** Informationen zum Laufwerk für die Installation des Programms und zu dem für die Installation benötigten freien Speicherplatz in der Datenträgerumgebung sorgfältig durch.

Um das Programm mit den Standard-Installationsparametern zu installieren, klicken Sie auf die Schaltfläche **Installieren**, und geben Sie das Administratorkennwort zur Bestätigung ein.

Um ein anderes Laufwerk zur Installation des Programms auszuwählen, klicken Sie auf die Schaltfläche **Ort für die Installation ändern**, und wählen Sie ein anderes Laufwerk aus. Klicken Sie abschließend auf die Schaltfläche **Fortfahren**.

Das Laufwerk für die Installation des Programms soll ein Boot-Laufwerk sein. Auf dem Laufwerk soll das Betriebssystem der Version nicht älter als die in den Systemvoraussetzungen angegebene Version installiert sein (s. Abschnitt "Hard- und Softwarevoraussetzungen" auf Seite 20).

Warten Sie, bis das Installationsprogramm für Kaspersky Anti-Virus die Programmkomponenten installiert hat.

8. Lesen Sie Informationen zum Abschluss des Installationsvorgangs im Fenster **Zusammenfassung** durch, und klicken Sie auf die Schaltfläche **Schließen**, um das Installationsprogramm zu beenden.

Nach Fertigstellung der Installation wird Kaspersky Anti-Virus automatisch gestartet. Ein Neustart des Computers ist nicht erforderlich.

BENUTZERDEFINIERTE INSTALLATION VON KASPERSKY ANTI-VIRUS

Um die benutzerdefinierte Installation von Kaspersky Anti-Virus auszuführen, gehen Sie folgendermaßen vor:

1. Öffnen Sie die mitgelieferten Dateien von Kaspersky Anti-Virus. Legen sie dafür die Installations-CD ins Laufwerk.

Wenn Sie Kaspersky Anti-Virus im Online-Shop gekauft haben, ist auf der Webseite von Kaspersky Lab das Programm im zip-Format zum Download erhältlich. Entpacken Sie es und starten Sie die Datei .dmg, um die mitgelieferten Dateien zu sehen.

2. Starten Sie das Installationsprogramm von Kaspersky Anti-Virus. Öffnen Sie dafür im Fenster mit dem Distributionsinhalt das Installationspaket **Kaspersky Anti-Virus 2011**.

   Bestätigen Sie den Start des Installationsprogramms im Bestätigungsfenster. Befolgen Sie die Schritte des Installationsprogramms, um das Programm zu installieren.

3. Klicken Sie im Fenster **Einführung** auf die Schaltfläche **Fortfahren**.

4. Lesen Sie danach im Fenster **Bitte lesen** die Informationen zu dem zu installierenden Programm durch.

   Vergewissern Sie sich, dass Ihr Computer die angegebenen Systemvoraussetzungen erfüllt. Um die Informationen auszudrucken, klicken Sie auf die Schaltfläche **Drucken**. Um die Daten in einer Textdatei zu sichern, klicken Sie auf die Schaltfläche **Sichern**. Zum Fortsetzen der Installation klicken Sie auf die Schaltfläche **Fortsetzen**.

5. Machen Sie sich im Fenster **Lizenz** mit der Lizenzvereinbarung zur Nutzung von Kaspersky Anti-Virus vertraut, die zwischen Ihnen und Kaspersky Lab ZAO abgeschlossen wird. Der Text der Vereinbarung ist in verschiedenen Sprachen verfügbar. Um die Lizenzvereinbarung auszudrucken, klicken Sie auf die Schaltfläche **Drucken**. Um die Vereinbarung in einer Textdatei zu sichern, klicken Sie auf die Schaltfläche **Sichern**.

   Wenn Sie mit allen Punkten in der Vereinbarung einverstanden sind, klicken Sie auf die Schaltfläche **Fortfahren**. Daraufhin erscheint das Bestätigungsfenster für Ihre Zustimmung zu den Bedingungen der Lizenzvereinbarung. Sie können folgende Aktionen ausführen:

   - Fortsetzen der Installation von Kaspersky Anti-Virus. Klicken Sie dazu auf die Schaltfläche **Akzeptieren**.
   - Zur Lizenzvereinbarung zurückkehren. Klicken Sie dazu auf die Schaltfläche **Lizenz lesen**.
   - Installation des Programms abbrechen. Klicken Sie dazu auf die Schaltfläche **Ablehnen**.

6. Lesen Sie im Fenster **KSN** die Informationen über die Teilnahme an Kaspersky Security Network durch (s. Abschnitt "An Kaspersky Security Network teilnehmen" auf Seite 102). Eine Beteiligung an diesem Programm sieht vor, dass Informationen über auf Ihrem Computer erkannte neue Bedrohungen, über gestartete Programme und über geladene signierte Programme an Kaspersky Lab geschickt werden. Außerdem werden ein einmaliger Identifikator, der Ihrem Exemplar von Kaspersky Anti-Virus zugewiesen wurde, sowie Systeminformationen gesendet. Es wird dabei garantiert, dass keine persönlichen Daten gesendet werden.

   Wenn Sie mit allen Punkten der Bestimmung über die Verwendung von Kaspersky Security Network einverstanden sind, aktivieren Sie das Kontrollkästchen **Ich akzeptiere die Teilnahmebedingungen an KSN**. Zum Fortsetzen der Installation klicken Sie auf die Schaltfläche **Fortsetzen**.

   Sie können jederzeit Ihre Teilnahme an Kaspersky Security Network verweigern (s. Abschnitt "An Kaspersky Security Network teilnehmen" auf Seite 102).

7. Lesen Sie im Fenster **Installationstyp** Informationen zum Laufwerk für die Installation des Programms und zu dem für die Installation benötigten freien Speicherplatz in der Datenträgerumgebung sorgfältig durch.

   Um ein anderes Laufwerk zur Installation des Programms auszuwählen, klicken Sie auf die Schaltfläche **Ort für die Installation ändern**, und wählen Sie ein anderes Laufwerk aus. Klicken Sie abschließend auf die Schaltfläche **Fortfahren**.

   Das Laufwerk für die Installation des Programms soll ein Boot-Laufwerk sein. Auf dem Laufwerk soll das Betriebssystem der Version nicht älter als die in den Systemvoraussetzungen angegebene Version installiert sein (s. Abschnitt "Hard- und Softwarevoraussetzungen" auf Seite 20).

   Klicken Sie auf die Schaltfläche **Anpassen**, um die Programmkomponenten für die benutzerdefinierte Installation auszuwählen.

8. Geben Sie im folgenden Fenster an, welche Programmkomponenten auf dem Computer installiert werden sollen. Deaktivieren Sie die Kontrollkästchen neben den Namen der Komponenten, die nicht installiert werden sollen.

   - **Virensuche**: Ermöglicht die Untersuchung von Objekten in benutzerdefinierten Bereichen.

     Diese Komponente von Kaspersky Anti-Virus wird immer installiert.

   - **Datei-Anti-Virus**: Untersucht in Echtzeit alle Dateien, die geöffnet, gestartet und gespeichert werden.

   - **Finder Kontextmenü**: Ermöglicht die Untersuchung von Objekten auf Viren, die im Finder-Kontextmenü angezeigt werden. Die Untersuchung wird über das Kontextmenü des Objekts gestartet.

   - **Modul zur Link-Untersuchung**. Ermöglicht die Untersuchung von Links in Browsern auf Sicherheit.

   Klicken Sie nach der Komponentenauswahl auf die Schaltfläche **Installieren**, und geben Sie das Administratorkennwort zur Bestätigung der Installation ein. Um zu den Standardeinstellungen der Installation zurückzukehren (s. Abschnitt "Standardinstallation von Kaspersky Anti-Virus" auf Seite 22), klicken Sie auf die Schaltfläche **Standardinstallation**.

   Warten Sie, bis das Installationsprogramm Kaspersky Anti-Virus die ausgewählten Programmkomponenten installiert hat.

9. Lesen Sie Informationen zum Abschluss des Installationsvorgangs im Fenster **Zusammenfassung** durch, und klicken Sie auf die Schaltfläche **Schließen**, um das Installationsprogramm zu beenden.

   Nach Fertigstellung der Installation wird Kaspersky Anti-Virus automatisch gestartet. Ein Neustart des Computers ist nicht erforderlich.

VORBEREITUNG ZUR NUTZUNG DES PROGRAMMS

Es wird empfohlen, nach der Programminstallation folgende Aktionen durchzuführen:

- Kaspersky Anti-Virus aktivieren (s. Abschnitt "Kaspersky Anti-Virus aktivieren" auf Seite 29). Die Verwendung einer lizenzierten Version erlaubt Ihnen, regelmäßig die Antiviren-Datenbanken zu aktualisieren, und bietet Ihnen Zugriff auf die Leistungen des technischen Supports.
- Aktuellen Schutzzustand einschätzen (siehe Abschnitt "Schutzstatus des Computers einschätzen" auf Seite 44), um sicherzustellen, dass Kaspersky Anti-Virus den Schutz auf der erforderlichen Stufe gewährleistet.
- Kaspersky Anti-Virus aktualisieren (siehe Abschnitt "Wie man die Datenbanken und Programm-Module aktualisiert" auf Seite 48). Damit Viren und andere schädliche Programme jederzeit erkannt und neutralisiert werden können, ist es erforderlich sicherzustellen, dass die Datenbanken von Kaspersky Anti-Virus stets aktuell sind.
- Vollständige Untersuchung des Computers ausführen (siehe Abschnitt "Computer vollständig auf Viren untersuchen" auf Seite 46).

Wenn Probleme oder Fehler im Programmbetrieb auftreten, öffnen Sie das Fenster der Betriebsberichte von Kaspersky Anti-Virus (siehe Abschnitt "Berichte" auf Seite 98). Möglicherweise können Sie den Grund der Störung dem Bericht entnehmen. Wenn es Ihnen nicht gelingt, das Problem selbst zu lösen, wenden Sie sich an den Technischen Support von Kaspersky Lab (siehe Abschnitt "Kontaktaufnahme mit dem Technischen Support" auf Seite 113).

PROGRAMM DEINSTALLIEREN

Nach der Deinstallation von Kaspersky Anti-Virus besteht ein ernsthaftes Infektionsrisiko für Ihren Computer.

Es wird empfohlen, vor der Deinstallation alle Objekte zu bearbeiten, die in der Quarantäne und im Backup gespeichert wurden. Alle unbearbeiteten Quarantäne- und Backup-Objekte werden unwiderruflich gelöscht.

Um Kaspersky Anti-Virus von Ihrem Computer zu deinstallieren, gehen Sie folgendermaßen vor:

1. Öffnen Sie die mitgelieferten Dateien von Kaspersky Anti-Virus. Legen sie dafür die Installations-CD ins Laufwerk.

   Wenn Sie Kaspersky Anti-Virus im Online-Shop gekauft haben, ist auf der Webseite von Kaspersky Lab das Programm im zip-Format zum Download erhältlich. Entpacken Sie es und starten Sie die Datei .dmg, um die mitgelieferten Dateien zu sehen.

2. Starten Sie das Deinstallationsprogramm von Kaspersky Anti-Virus. Wählen Sie dazu im Fenster mit den mitgelieferten Dateien **Kaspersky Anti-Virus 2011 deinstallieren** aus.

   Befolgen Sie die Schritte des Deinstallationsprogramms, um Kaspersky Anti-Virus zu deinstallieren.

3. Klicken Sie im Fenster **Einleitung** auf die Schaltfläche **Fortfahren**.

4. Lesen Sie wichtige Informationen im Fenster **Information** durch. Um den Deinstallationsvorgang zu starten, klicken Sie auf die Schaltfläche **Löschen** und geben das Administratorkennwort zur Bestätigung der Deinstallation ein. Warten Sie, bis das Programm deinstalliert wurde.

5. Lesen Sie Informationen zum Abschluss des Deinstallationsvorgangs im Fenster **Abschluss von** durch, und klicken Sie auf die Schaltfläche **Fertig stellen**, um das Deinstallationsprogramm zu beenden.

   Ein Neustart des Computers ist nach der Deinstallation von Kaspersky Anti-Virus nicht erforderlich.

LIZENZVERWALTUNG

Dieser Abschnitt informiert über die wichtigsten Begriffe, die mit der Programmlizenzierung zusammenhängen. Hier können Sie erfahren, wie das Programm aktiviert wird und wo Sie die Informationen zur aktuellen Lizenz ansehen können. Außerdem finden Sie hier Informationen darüber, wie Sie eine Lizenz erwerben und ihre Gültigkeitsdauer verlängern können.

IN DIESEM ABSCHNITT

Über die Lizenz 26

Lizenz-Info anzeigen 27

Lizenz erwerben 27

Lizenz verlängern 28

Über den Lizenzvertrag 29

Über den Aktivierungscode 29

Über den Lizenzschlüssel 29

Kaspersky Anti-Virus aktivieren 29

ÜBER DIE LIZENZ

Als *Lizenz* wird ein Recht zur Nutzung von Kaspersky Anti-Virus und entsprechenden Zusatzleistungen bezeichnet, die Ihnen Kaspersky Lab oder ein Händler von Kaspersky Lab zur Verfügung stellt.

Jede Lizenz weist eine Gültigkeitsdauer und einen Typ auf.

Die *Gültigkeitsdauer einer Lizenz* ist die Zeitspanne, für die Ihnen die Zusatzleistungen zur Verfügung stehen:

- technischer Support
- Update der Datenbanken und Module des Programms.

Der Umfang der verfügbaren Leistungen hängt von dem Typ der Lizenz ab.

Die folgenden Lizenztypen sind vorgesehen:

- *Test*: Das ist eine kostenlose Lizenz mit einer beschränkten Gültigkeitsdauer (z.B. 30 Tage), die dazu dient, den Benutzer in Kaspersky Anti-Virus einzuführen.

  Eine Testlizenz darf nur einmal benutzt werden.

  Wenn Sie über eine Testlizenz verfügen, können Sie sich nur bei Fragen zur Programmaktivierung oder zum Kauf einer kommerziellen Lizenz an den technischen Support wenden. Nach Ablauf der Testlizenz führt Kaspersky Anti-Virus keine Funktionen mehr aus. Um die Arbeit mit dem Programm fortzusetzen, muss das Programm aktiviert werden (siehe Abschnitt "Kaspersky Anti-Virus aktivieren" auf Seite 29).

- *Kommerzielle* – gebührenpflichtige Lizenz mit begrenzter Gültigkeitsdauer (zum Beispiel ein Jahr).

  Während der Gültigkeitsdauer einer kommerziellen Lizenz sind alle Funktionen des Programms sowie Zusatzleistungen verfügbar.

Nach Ablauf der Gültigkeitsdauer der kommerziellen Lizenz bleibt die volle Funktionalität von Kaspersky Anti-Virus erhalten. Die Datenbanken werden jedoch nicht aktualisiert. Sie können Ihren Computer weiterhin untersuchen und die Schutzkomponenten verwenden, allerdings nur mit den Datenbanken, die bei Ablauf der Lizenz aktuell waren. Um eine Infektion Ihres Computers durch neue Viren zu verhindern, empfehlen wir Ihnen, die Lizenz für die Nutzung der Anwendung zu verlängern.

Nachdem Sie das Programm mit einer kommerziellen Lizenz aktiviert haben, können Sie eine Reservelizenz für Kaspersky Anti-Virus erwerben und aktivieren. In diesem Fall wird der Reservelizenz nach Ablauf der Gültigkeitsdauer der aktiven Lizenz der Status der aktiven Lizenz zugewiesen, und die Ausführung des Programms wird ohne Änderungen fortgesetzt. Kaspersky Anti-Virus kann nur über eine Reservelizenz verfügen.

LIZENZ-INFO ANZEIGEN

- *Um die Informationen zur aktiven Lizenz zu sehen,*

  Öffnen Sie das Programmhauptfenster (siehe Seite 34), und klicken Sie auf die Schaltfläche .

Das folgende Fenster (siehe Abbildung unten) bietet folgende Informationen zur Lizenz an: Nummer, Typ (kommerziell, Test), Beschränkung der Anzahl der Computer, für die die Lizenz gültig ist, Gültigkeitsende (Datum und Uhrzeit), Anzahl der verbleibenden Tage.

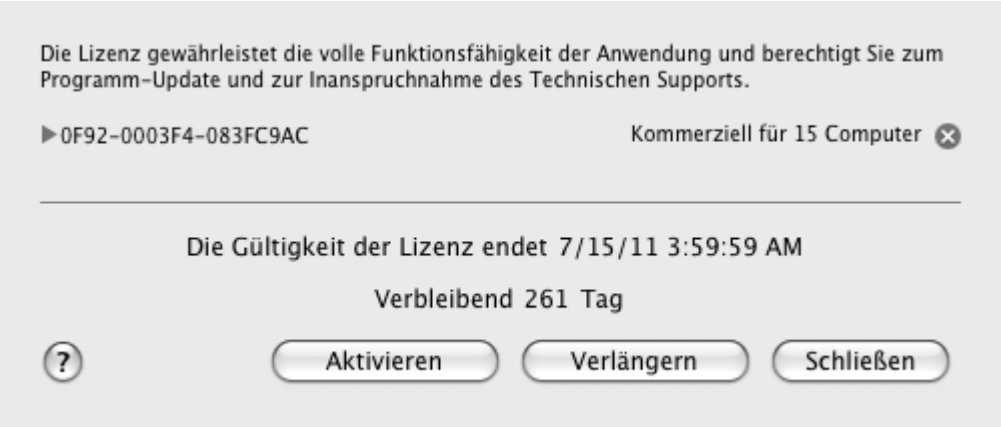
Die Lizenz gewährleistet die volle Funktionsfähigkeit der Anwendung und berechtigt Sie zum Programm-Update und zur Inanspruchnahme des Technischen Supports.
0F92-0003F4-083FC9AC
Kommerziell für 15 Computer
Die Gültigkeit der Lizenz endet 7/15/11 3:59:59 AM
Verbleibend 261 Tag
Aktivieren
Verlängern
Schließen

Abbildung 1. Lizenzverwaltung

Wenn keine Lizenz vorhanden ist, benachrichtigt Sie Kaspersky Anti-Virus darüber. Wenn das Programm nicht aktiviert ist, können Sie den Vorgang zur Aktivierung starten (siehe Abschnitt "Aktivierung von Kaspersky Anti-Virus" auf Seite 29). Wenn eine Testversion des Programms aktiviert wurde, können Sie eine kommerzielle Lizenz erwerben (s. Abschnitt "Lizenz erwerben" auf Seite 27). Wenn die Gültigkeitsdauer der kommerziellen Lizenz bald abläuft, können Sie sie verlängern (siehe Abschnitt "Lizenz verlängern" auf Seite 28).

LIZENZ ERWERBEN

- *Um eine neue Lizenz zu erwerben, gehen Sie folgendermaßen vor:*

  1. Öffnen Sie das Programmhauptfenster (siehe Seite 34), und klicken Sie auf die Schaltfläche .
  2. Klicken Sie im folgenden Fenster (siehe Abbildung unten) auf die Schaltfläche **Kaufen**.

Dadurch wird eine Webseite geöffnet, auf der Sie umfassende Informationen darüber finden, zu welchen Bedingungen Sie im Internet-Shop von Kaspersky Lab oder bei einem autorisierten Händler eine Lizenz erwerben können. Beim Kauf über einen Internet-Shop wird Ihnen nach Zahlungseingang per E-Mail an die im Bestellformular angegebene Adresse ein Aktivierungscode für Kaspersky Anti-Virus (siehe Abschnitt "Über den Aktivierungscode" auf Seite 29) zugeschickt.

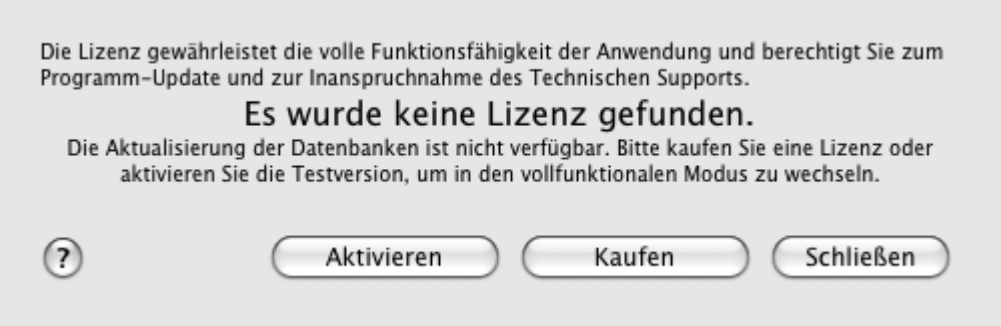
Die Lizenz gewährleistet die volle Funktionsfähigkeit der Anwendung und berechtigt Sie zum Programm-Update und zur Inanspruchnahme des Technischen Supports.
Es wurde keine Lizenz gefunden.
Die Aktualisierung der Datenbanken ist nicht verfügbar. Bitte kaufen Sie eine Lizenz oder aktivieren Sie die Testversion, um in den vollfunktionalen Modus zu wechseln.
?
Aktivieren
Kaufen
Schließen

Abbildung 2. Lizenz erwerben

LIZENZ VERLÄNGERN

Es ist erforderlich, die Lizenz zu verlängern, wenn die Gültigkeitsdauer der vorhandenen Lizenz abgelaufen ist. In diesem Fall führt Kaspersky Anti-Virus alle seine Funktionen weiterhin aus, allerdings werden die Antiviren-Datenbanken nicht mehr aktualisiert.

Um das Recht zur Nutzung der vorhandenen Lizenz zu verlängern, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Programmhauptfenster (siehe Seite 34), und klicken Sie auf die Schaltfläche .
2. Klicken Sie im folgenden Fenster (siehe Abbildung unten) auf die Schaltfläche **Verlängern**.

Dadurch wird eine Webseite geöffnet, auf der Sie umfassende Informationen darüber finden, zu welchen Bedingungen Sie im Internet-Shop von Kaspersky Lab oder bei einem autorisierten Händler die Gültigkeitsdauer der Lizenz verlängern können. Bei Verlängerung über einen Internet-Shop wird Ihnen nach Zahlungseingang per E-Mail an die im Bestellformular angegebene Adresse ein Aktivierungscode für Kaspersky Anti-Virus (siehe Abschnitt "Über den Aktivierungscode" auf Seite 29) zugeschickt.

Kaspersky Lab bietet regelmäßig Sonderangebote zu den Lizenzen für unsere Produkte an. Verfolgen Sie unsere Aktionen auf der Webseite von Kaspersky Lab im Abschnitt **Produkte → Aktionen und Sonderangebote**.

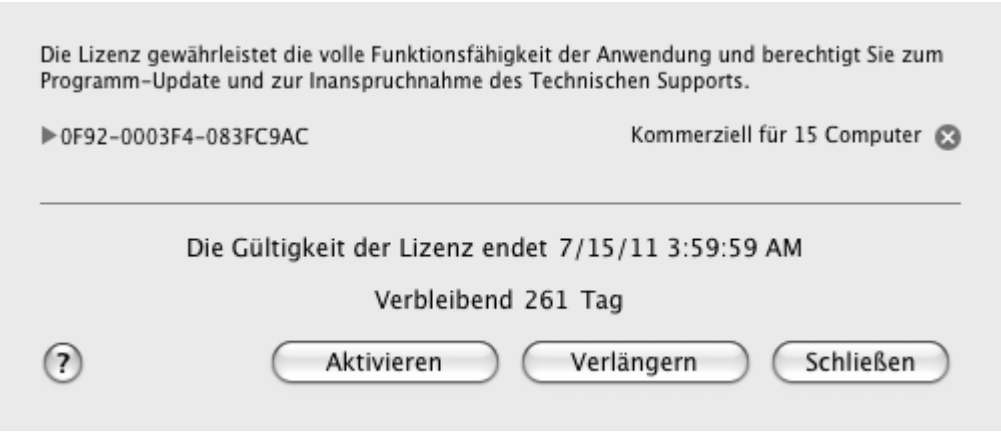
Die Lizenz gewährleistet die volle Funktionsfähigkeit der Anwendung und berechtigt Sie zum Programm-Update und zur Inanspruchnahme des Technischen Supports.
▶0F92-0003F4-083FC9AC
Kommerziell für 15 Computer
Die Gültigkeit der Lizenz endet 7/15/11 3:59:59 AM
Verbleibend 261 Tag
?
Aktivieren
Verlängern
Schließen

Abbildung 3. Lizenzverwaltung

ÜBER DEN LIZENZVERTRAG

Der *Lizenzvertrag* ist ein Vertrag zwischen einer natürlichen oder juristischen Person, die rechtmäßiger Besitzer eines Exemplars von Kaspersky Anti-Virus ist, und der Kaspersky Lab ZAO. Der Lizenzvertrag gehört zum Lieferumfang jedes Kaspersky-Lab-Programms. Er legt die Rechte und Einschränkungen für die Nutzung von Kaspersky Anti-Virus genau fest.

ÜBER DEN AKTIVIERUNGSCODE

Ein *Aktivierungscode* ist ein Code, den Sie beim Kauf einer kommerziellen Lizenz für Kaspersky Anti-Virus erhalten. Dieser Code ist für die Programmaktivierung erforderlich.

Der Aktivierungscode besteht aus einer durch Bindestriche getrennten Folge von lateinischen Buchstaben und Ziffern, die in vier Blöcken zu je fünf Zeichen angeordnet sind (Beispiel: AA111-AA111-AA111-AA111).

ÜBER DEN LIZENZSCHLÜSSEL

Die Möglichkeit zur Nutzung von Kaspersky Anti-Virus wird durch das Vorhandensein einer *Schlüsseldatei* bestimmt. Den Lizenzschlüssel erhalten Sie anhand des Aktivierungscodes (siehe Abschnitt "Über den Aktivierungscode" auf Seite 29), den Sie beim Kauf des Programms erworben haben. Der Lizenzschlüssel berechtigt Sie zur Nutzung des Programms ab dem Tag der Installation. Der Schlüssel enthält Informationen zur Lizenz: Typ, Gültigkeitsdauer und Anzahl der Computer, für die die Lizenz gültig ist.

KASPERSKY ANTI-VIRUS AKTIVIEREN

Vergewissern Sie sich vor der Aktivierung von Kaspersky Anti-Virus, dass Datum und Uhrzeit des Computers korrekt eingestellt sind.

Der Vorgang zur Aktivierung des Programms besteht in der Installation einer Schlüsseldatei (siehe Abschnitt "Über die Schlüsseldatei" auf Seite 29), auf deren Grundlage Kaspersky Anti-Virus das Vorhandensein der Rechte zur Nutzung des Programms überprüft und die Nutzungsdauer ermittelt.

Das Programm wird mithilfe des Aktivierungsassistenten aktiviert. Befolgen Sie die Schritte des Assistenten, um das Programm zu aktivieren.

In einem beliebigen Schritt des Aktivierungsassistenten können Sie die Aktivierung des Programms durch Klicken auf die Schaltfläche **Abbrechen** vorübergehend aufschieben. Dadurch wird der Aktivierungsassistent beendet. Wenn das Programm nicht aktiviert ist, können Sie alle Funktionen von Kaspersky Anti-Virus außer dem Update nutzen. Sie können das Programm nur einmal nach der Installation updaten.

IN DIESEM ABSCHNITT

Testversion aktivieren 30

Programm mithilfe des Aktivierungscodes aktivieren 30

Programm mithilfe der Schlüsseldatei aktivieren 31

TESTVERSION AKTIVIEREN

Die Aktivierung einer Testversion wird vom Aktivierungsassistenten nur in dem Fall angeboten, wenn diese Version von Kaspersky Anti-Virus noch nicht vorher auf diesem Computer installiert wurde.

Wählen Sie diese Aktivierungsvariante, wenn Sie eine Testversion des Programms verwenden möchten, bevor Sie sich über den Kauf einer kommerziellen Version entscheiden. Sie erhalten einen kostenlosen Schlüssel, dessen Gültigkeitsdauer durch die Testlizenz beschränkt ist.

Bei der Aktivierung einer Testversion ist eine Internetverbindung erforderlich. Ist momentan keine Internetverbindung vorhanden, kann die Aktivierung später vorgenommen werden.

Um eine Testversion des Programms zu aktivieren, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Programmhauptfenster (siehe Seite 34), und klicken Sie auf die Schaltfläche .
2. Klicken Sie im folgenden Fenster auf **Aktivieren**. Daraufhin wird der Aktivierungsassistent aufgerufen. Befolgen Sie die Schritte des Assistenten, um das Programm zu aktivieren.
3. Wählen Sie im Fenster **Aktivierungsmethode** die Aktivierungsmethode für das Programm **Testversion aktivieren** aus.
4. Warten Sie bis der Aktivierungsassistent im Fenster **Schlüsseldatei herunterladen** eine Verbindung mit den Servern des Kaspersky Lab herstellt und die Angaben zur Prüfung sendet. Bei erfolgreicher Prüfung erhält und installiert der Assistent eine Schlüsseldatei mit der Geltungsdauer, die durch die Testlizenz begrenzt ist.

   Wenn die Gültigkeit der Testlizenz für diese Programmversion abgelaufen ist, erscheint eine entsprechende Meldung auf dem Bildschirm.
5. Der Aktivierungsassistent informiert Sie über den erfolgreichen Abschluss des Aktivierungsvorgangs im Fenster **Informationen zur Schlüsseldatei**. Außerdem werden folgende Informationen über den installierten Schlüssel angezeigt: Nummer, Typ (Test) und Gültigkeit des Schlüssels. Klicken Sie auf die Schaltfläche **Fertig**, um den Assistenten abzuschließen.

PROGRAMM MITHILFE DES AKTIVIERUNGSCODES AKTIVIEREN

Verwenden Sie diese Aktivierungsmethode, wenn Sie eine kommerzielle Programmversion erworben und einen Aktivierungscode erhalten haben. Auf Grundlage dieses Codes erhalten Sie die Schlüsseldatei, die einen Zugang zu den Funktionen von Kaspersky Anti-Virus für die Geltungsdauer der Testlizenz sicherstellt.

Bei Auswahl der Anwendungsaktivierung per Aktivierungscode ist eine Internetverbindung erforderlich. Ist momentan keine Internetverbindung vorhanden, kann die Aktivierung später vorgenommen werden.

Um das Programm mithilfe eines Aktivierungscodes zu aktivieren, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Programmhauptfenster (siehe Seite 34), und klicken Sie auf die Schaltfläche .
2. Klicken Sie im folgenden Fenster auf **Aktivieren**. Daraufhin wird der Aktivierungsassistent aufgerufen. Befolgen Sie die Schritte des Assistenten, um das Programm zu aktivieren.
3. Wählen Sie im Fenster **Aktivierungsmethode** die Aktivierungsmethode **Mit Aktivierungscode aktivieren** aus.
4. Geben Sie im Fenster **Aktivierungscode eingeben** den Aktivierungscode ein, den Sie beim Kauf von Kaspersky Anti-Virus erhalten haben.

Der Aktivierungscode besteht aus einer durch Bindestriche getrennten Folge von Ziffern und Buchstaben, die in vier Blöcke zu je fünf Zeichen unterteilt ist und keine Leerzeichen enthält. Beispiel: 11AA1-11AAA-1AA11-1A111. Beachten Sie, dass der Code in lateinischen Buchstaben eingegeben werden muss.

5. Warten Sie bis der Aktivierungsassistent im Fenster **Schlüsseldatei herunterladen** eine Verbindung mit den Servern des Kaspersky Lab herstellt und die Angaben zur Prüfung sendet. Bei erfolgreicher Überprüfung des Aktivierungscodes erhält der Assistent eine Schlüsseldatei.

   Kaspersky Anti-Virus erhält vom Server nicht die physische Datei mit der Endung .key, sondern die Information, die im Operationssystem gespeichert ist. Um die echte Schlüsseldatei zu erhalten, muss man eine Benutzerregistrierung auf der Webseite von Kaspersky Lab durchführen (http://www.kaspersky.de/support).

   Wenn der Aktivierungscode die Überprüfung nicht besteht, erscheint eine entsprechende Meldung auf dem Bildschirm. Wenden Sie sich in diesem Fall an die Firma, bei der Sie Kaspersky Anti-Virus gekauft haben.

6. Der Aktivierungsassistent informiert Sie über den erfolgreichen Abschluss des Aktivierungsvorgangs im Fenster **Informationen zur Schlüsseldatei**. Außerdem werden folgende Informationen über den installierten Schlüssel angezeigt: Nummer, Typ (kommerziell) und Gültigkeit des Schlüssels. Klicken Sie auf die Schaltfläche **Fertig**, um den Assistenten abzuschließen.

PROGRAMM MITHILFE DER SCHLÜSSELDATEI AKTIVIEREN

Verwenden Sie diese Variante, um das Programm mit einer bereits vorhandenen Schlüsseldatei zu aktivieren.

Bei Aktivierung mithilfe einer Schlüsseldatei ist keine Internetverbindung erforderlich. Es wird empfohlen, diese Aktivierungsmethode zu verwenden, wenn die Internetverbindung nicht möglich oder vorübergehend nicht verfügbar ist.

➧ *Um das Programm mit Hilfe der vorher erhaltenen Schlüsseldatei zu aktivieren, führen Sie folgende Aktionen durch:*

1. Öffnen Sie das Programmhauptfenster (siehe Seite 34), und klicken Sie auf die Schaltfläche .

2. Klicken Sie im folgenden Fenster auf **Aktivieren**. Daraufhin wird der Aktivierungsassistent aufgerufen. Befolgen Sie die Schritte des Assistenten, um das Programm zu aktivieren.

3. Wählen Sie im Fenster **Aktivierungsmethode** die Aktivierungsmethode **Vorherigen Schlüsseldatei verwenden** aus.

4. Klicken Sie im Fenster **Schlüsseldatei wählen** auf die Schaltfläche **Wählen**, und wählen Sie im folgenden Fenster die Schlüsseldatei mit der Endung key aus. Daraufhin werden im unteren Bereich des Fensters Informationen über den verwendeten Schlüssel angezeigt: Nummer, Typ (kommerziell) und Gültigkeit des Schlüssels.

5. Der Aktivierungsassistent informiert Sie über den erfolgreichen Abschluss des Aktivierungsvorgangs im Fenster **Informationen zur Schlüsseldatei**. Außerdem werden folgende Informationen über den installierten Schlüssel angezeigt: Nummer, Typ und Gültigkeit des Schlüssels. Klicken Sie auf die Schaltfläche **Fertig**, um den Assistenten abzuschließen.

PROGRAMMOBERFLÄCHE

Dieser Abschnitt beschreibt die wichtigsten Elemente der grafischen Programmoberfläche: Symbol und Kontextmenü des Programms, Hauptfenster, Konfigurationsfenster und Meldungsfenster.

IN DIESEM ABSCHNITT

Symbol von Kaspersky Anti-Virus 32

Programmhauptfenster 34

Programmkonfigurationsfenster 35

Meldungsfenster und Pop-up-Meldungen 36

Oberfläche von Kaspersky Anti-Virus anpassen 39

SYMBOL VON KASPERSKY ANTI-VIRUS

Sofort nach der Installation von Kaspersky Anti-Virus erscheint in der Menüleiste das Programmsymbol. Das Symbol dient als Indikator für die Aktivität des Programms. Wenn das Symbol aktiv ist, ist der Schutz des Dateisystems Ihres Computers vor schädlichen Programmen in Echtzeit aktiviert. Ein inaktives Symbol deutet darauf hin, dass der Schutz ausgeschaltet ist. Außerdem können Sie über das Kontextmenü des Symbols auf die folgenden Grundbefehle von Kaspersky Anti-Virus zugreifen: Schutz des Computer-Dateisystems deaktivieren/fortsetzen, Update-Aufgaben und Aufgaben zur schnellen Untersuchung des Computers starten, in das Programmkonfigurationsfenster wechseln usw.

Standardmäßig befindet sich das Symbol in der Menüleiste. Sie können die Einstellungen für das Programm so anpassen, dass das Symbol von Kaspersky Anti-Virus in der Schnellstartleiste (Dock) angezeigt wird.

- *Damit das Programmsymbol in der Dock-Schnellstartleiste angezeigt wird Dock-Schnellstartleiste angezeigt wird, gehen Sie folgendermaßen vor:*

  1. Öffnen Sie das Programmkonfigurationsfenster (auf Seite 35), und wählen Sie die Registerkarte **Ansicht** aus (siehe Abbildung unten).

  2. Wählen Sie im Abschnitt **Programmsymbol anzeigen** die Variante **Im Dock** aus.

Beachten Sie, dass das Ändern dieses Parameters nur nach einem Neustart von Kaspersky Anti-Virus wirksam wird.

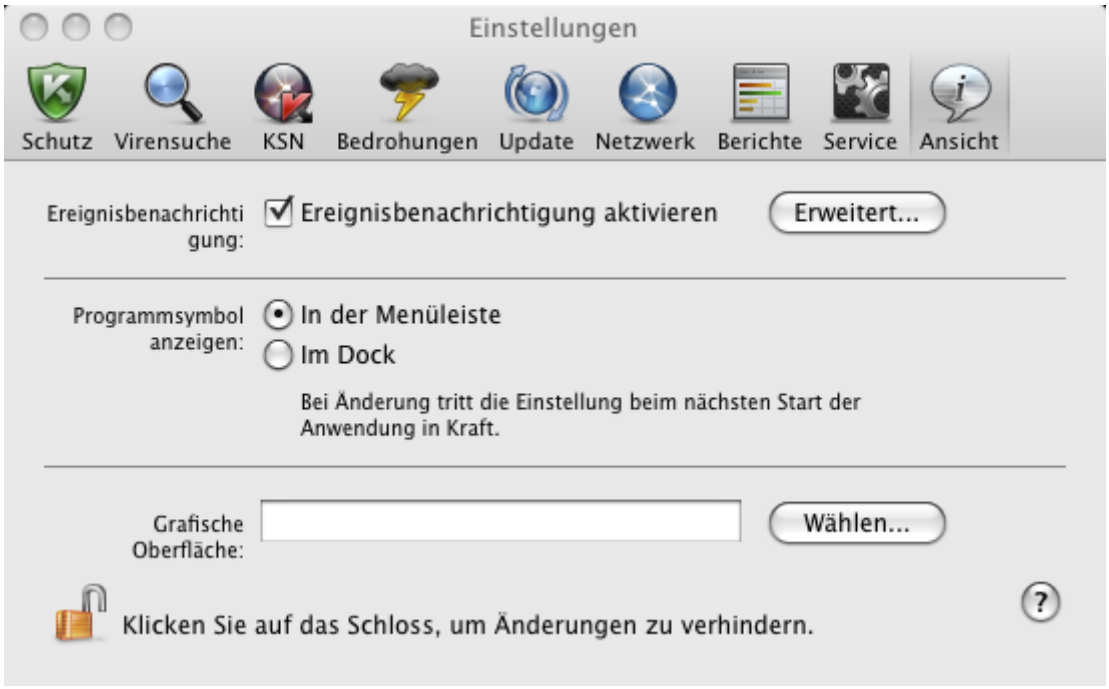

Abbildung 4. Programmkonfigurationsfenster. Ansicht

Wenn Sie die Anzeige des Symbols in der Menüleiste ausgewählt haben, erscheint das Symbol beim Programmstart oder beim Öffnen des Programmhauptfensters im Dock nicht. Sie können auch nicht mithilfe der Tastenkombination **Command-Tab** auf das Programm umschalten.

Abbildung 5. Kontextmenü des Symbols von Kaspersky Anti-Virus in der Menüleiste

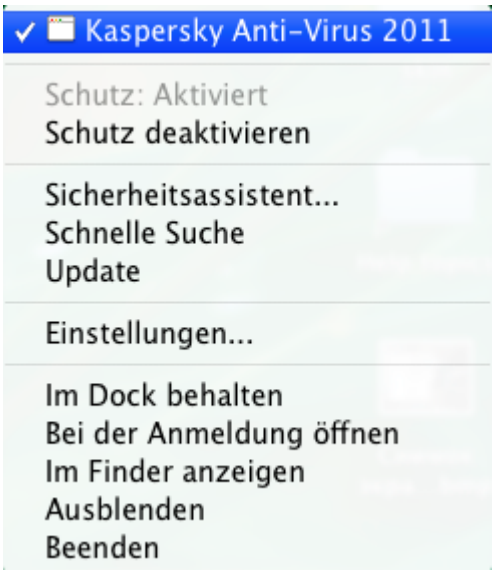

Abbildung 6. Kontextmenü des Symbols von Kaspersky Anti-Virus im Dock

PROGRAMMHAUPTFENSTER

- *Um das Programmhauptfenster zu öffnen,*

  klicken Sie auf das Symbol von Kaspersky Anti-Virus im Dock oder in der Dock-Menüleiste (siehe Abbildung oben) und wählen Sie im folgenden Menü den Befehl **Kaspersky Anti-Virus**.

Die wichtigste Aufgabe des Hauptfensters von Kaspersky Anti-Virus (siehe Abbildung unten) besteht darin, den Benutzer über den Zustand des Computerschutzes und über vorhandene Probleme zu informieren, Informationen über die Arbeit der Programmkomponenten (Datei-Antivirus, Untersuchungs- und Update-Aufgaben) bereitzustellen sowie den Zugriff auf die wichtigsten Aufgaben und das Programmkonfigurationsfenster zu gewähren.

Abbildung 7. Hauptfenster von Kaspersky Anti-Virus 2011

Es existieren drei Möglichkeiten für den Schutzstatus (siehe Abschnitt "Schutzstatus des Computers einschätzen" auf Seite 44). Jeder Zustand wird durch eine bestimmte Farbe gekennzeichnet. Die Farben entsprechen den Signalen einer Verkehrsampel. Der aktuelle Schutzstatus wird durch die Farbe des Indikators im Hauptfenster signalisiert. Grün bedeutet, dass der Schutz Ihres Computers dem erforderlichen Niveau entspricht. Gelb und Rot signalisieren, dass in den Einstellungen oder bei der Arbeit von Kaspersky Anti-Virus bestimmte Probleme vorliegen. Um ausführliche Informationen über die Probleme zu erhalten und sie schnell zu beheben, verwenden Sie den Sicherheitsassistenten (siehe Abschnitt "Sicherheitsassistent " auf Seite 45), der durch Klicken auf den farbigen Indikator geöffnet wird.

Im linken Bereich des Hauptfensters wird der Farbindikator durch Textinformationen über den Schutzstatus des Computers ergänzt und es werden Sicherheitsrisiken genannt, falls der Sicherheitsassistent solche erkannt hat. Außerdem werden auf der linken Seite des Hauptfensters Informationen über die Ausführung laufender Untersuchungs- oder Updateaufgaben (mit Prozentangabe) angezeigt.

Im unteren Bereich des Fensters befindet sich eine zusammenfassende Statistik über die Arbeit von Datei-Anti-Virus sowie Informationen über die verwendeten Programm-Datenbanken.

Direkt vom Hauptfenster aus können Sie das Update von Kaspersky Anti-Virus ausführen, Aufgaben zur Virensuche in bestimmten Bereichen starten und zur Verwaltung von Lizenzen gelangen. Verwenden Sie dazu die folgenden Schaltflächen:

Update von Kaspersky Anti-Virus starten: Nach Abschluss des Update-Vorgangs werden Detaildaten zur Aufgabenausführung im Berichtsfenster (siehe Abschnitt "Berichte" auf Seite 98) angezeigt.

Zu den Untersuchungsaufgaben **Schnelle Suche**, **Vollständige Suche** und **Virensuche** in dem durch den Benutzer vorgegebenen Bereich sowie zu allen benutzerdefinierten Untersuchungsaufgaben wechseln, wenn diese erstellt worden sind. Nach Abschluss der Untersuchung werden Detaildaten zur Aufgabenausführung im Berichtsfenster (siehe Abschnitt "Berichte" auf Seite 98) angezeigt.

Zu dem Fenster wechseln, in dem Informationen zur verwendeten Lizenz angezeigt werden.

Im oberen Bereich des Hauptfensters befindet sich eine Navigationsleiste, die folgende Schaltflächen enthält:

Das Berichtsfenster öffnen (siehe Abschnitt "Berichte" auf Seite 98) Kaspersky Anti-Virus, sowie Zugang zur Quarantäne (siehe Abschnitt "Quarantäne" auf Seite 93) und zum Backup erhalten (siehe Abschnitt "Backup" auf Seite 96).

Das Programmkonfigurationsfenster öffnen (siehe Seite 35).

Die elektronische Hilfe für Kaspersky Anti-Virus öffnen.

Ein Fenster mit Informationen über die Möglichkeiten, den technischen Support in Anspruch zu nehmen, öffnen(siehe Abschnitt "Kontaktaufnahme mit dem technischen Support" auf Seite 113).

PROGRAMMKONFIGURATIONSFENSTER

Das Konfigurationsfenster für Kaspersky Anti-Virus (siehe Abbildung unten) können Sie auf folgende Weise öffnen:

- durch Klicken auf die Schaltfläche im Programmhauptfenster (siehe Abschnitt "Programmhauptfenster" auf Seite 34);
- durch Auswahl des Befehls **Einstellungen** im Kontextmenü, das sich durch Klicken auf das Symbol von Kaspersky Anti-Virus (auf Seite 32) im Dock oder in der Menüleiste öffnet.

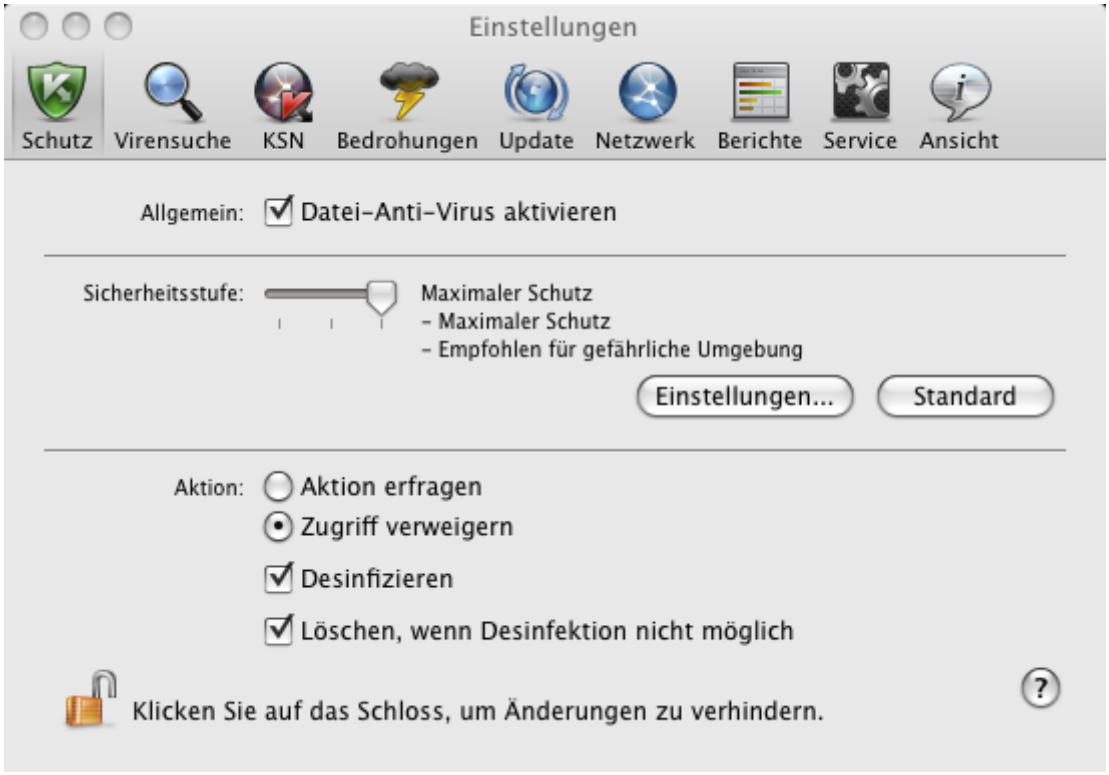

Abbildung 8. Programmkonfigurationsfenster. Schutz

Die Registerkarten im oberen Fensterbereich bieten schnellen Zugriff auf die folgenden Funktionen des Programms:

- Einstellungen von Datei-Anti-Virus;
- Einstellungen von Untersuchungsaufgaben;
- Einstellungen des Programm-Updates;
- Auswahl der zu kontrollierenden schädlichen Programme und Anlegen der vertrauenswürdigen Zone;
- Diensteinstellungen von Kaspersky Anti-Virus;
- Einstellungen für die Teilnahme an Kaspersky Security Network.

Die Feineinstellung bestimmter Parameter erfolgt in Konfigurationsfenstern der zweiten und dritten Ebene.

Um die Veränderung von Arbeitseinstellungen von Kaspersky Anti-Virus durch die Benutzer, die keine Administratorrechte besitzen, zu sperren, klicken Sie auf die Schaltfläche , die sich im unteren Teil des Fensters befindet. Um diese Sperre wieder aufzuheben, geben Sie die Benutzerdaten des Computeradministrators ein.

Die Schaltfläche bietet Zugriff auf das Hilfesystem von Kaspersky Anti-Virus mit einer Beschreibung der Parameter für das aktuelle Anwendungsfenster.

MELDUNGSFENSTER UND POP-UP-MELDUNGEN

Bei der Arbeit von Kaspersky Anti-Virus treten unterschiedliche Ereignisse ein. Sie können informativen Charakter aufweisen oder wichtige Angaben enthalten. Ein Ereignis kann beispielsweise über die erfolgreiche Aktualisierung des Programms informieren oder einen Fehler bei der Arbeit von Datei-Anti-Virus oder einer Untersuchungsaufgabe betreffen, der dringend behoben werden muss. Das Programm informiert Sie über das Eintreten von Ereignissen mit Hilfe von *Meldungsfenstern* und *Pop-up-Meldungen*.

IN DIESEM ABSCHNITT

Benachrichtigungen 37

Benachrichtigungsmethoden 37

Benachrichtigungen konfigurieren 38

Über Pop-up-Meldungen 39

BENACHRICHTIGUNGEN

Kaspersky Anti-Virus informiert während des Arbeitsvorgangs, wenn folgende Ereignistypen auftreten:

- **Kritische Ereignisse** – Ereignisse mit kritischer Priorität. Es wird ausdrücklich empfohlen, sich über solche Ereignisse benachrichtigen zu lassen, weil sie auf Probleme bei der Arbeit von Kaspersky Anti-Virus oder auf Schwachstellen im Schutz Ihres Computers hinweisen. Beispiele: *Programm-Datenbanken sind beschädigt* oder *Gültigkeit des Schlüssels ist abgelaufen*.

- **Funktionsstörung** – Ereignisse, die zur Funktionsunfähigkeit von Kaspersky Anti-Virus führen. Beispiele: *Programm-Datenbanken sind beschädigt*.

- **Wichtige Ereignisse** – Ereignisse, die unbedingt beachtet werden müssen. Beispiele: *Der Schutz wurde deaktiviert* oder *Der Computer wurde lange nicht auf Viren untersucht*.

- **Informative Ereignisse** – Ereignisse mit einem Hilfscharakter. Beispiele: *alle gefährliche Objekte wurden desinfiziert*.

Wenn Sie bei Ereignissen von Kaspersky Anti-Virus auf dem neuesten Stand bleiben wollen, machen Sie sich den Benachrichtigungsservice zunutze.

BENACHRICHTIGUNGSMETHODEN

Die Meldungen können durch die folgenden Methoden erfolgen:

- Pop-up-Meldungen

- Tonsignale.

Kaspersky Anti-Virus unterstützt das Benachrichtigungssystem Growl. Die Pop-up-Meldungen werden mittels Growl eingeblendet, wenn dieses System aktiviert ist.

BENACHRICHTIGUNGEN KONFIGURIEREN

Wenn Sie über Ereignisse benachrichtigt werden wollen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Programmkonfigurationsfenster (siehe Seite 35), und wählen Sie die Registerkarte **Ansicht** (siehe Abbildung unten) aus.

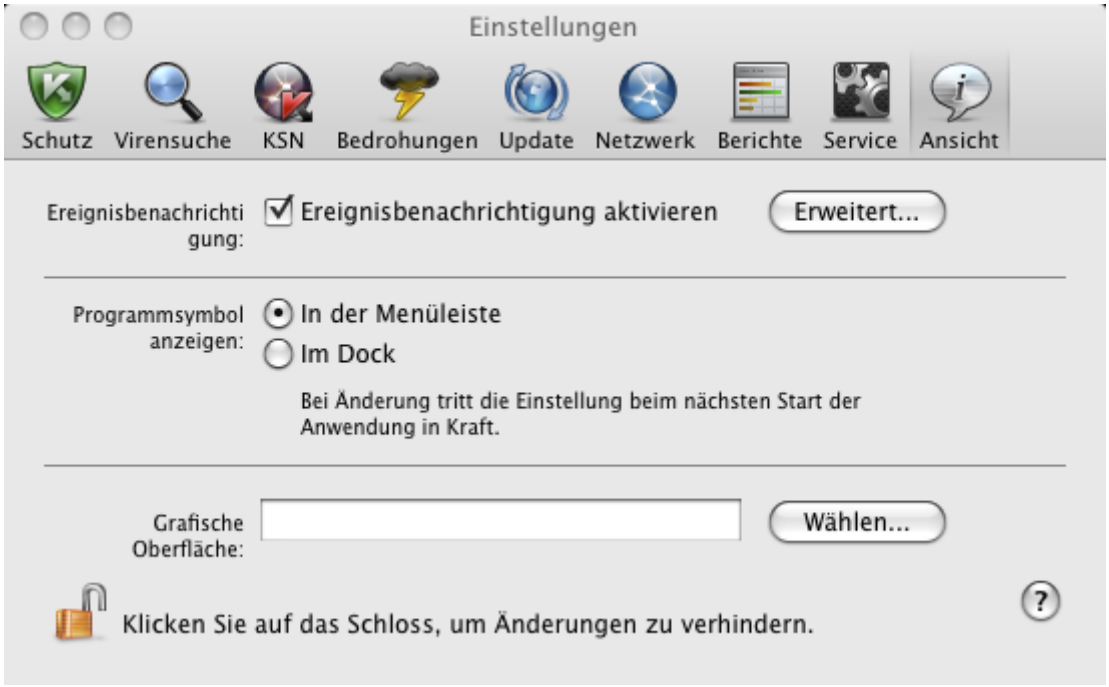

Abbildung 9. Programmkonfigurationsfenster. Ansicht

2. Aktivieren Sie das Kontrollkästchen **Ereignisbenachrichtigung aktivieren** im Block **Ereignisbenachrichtigung**, und wechseln Sie zur Feineinstellung. Klicken Sie dazu auf die Schaltfläche **Erweitert**.

Im folgenden Fenster (siehe Abbildung unten) können Sie folgende Benachrichtigungsmethoden für die oben genannten Ereignisse anpassen:

- *Popupmeldung*: Die Meldung enthält Informationen über das eingetretene Ereignis.

  Um diesen Typ der Benachrichtigung zu verwenden, aktivieren Sie das Kontrollkästchen in der Spalte **Anzeige** neben dem Ereignis, über das Sie benachrichtigt werden möchten.

- *Tonsignale*.

  Wenn Sie möchten, dass diese Benachrichtigung von einem Audiosignal begleitet wird, aktivieren Sie in der Spalte **Ton** das Kontrollkästchen für das Ereignis.

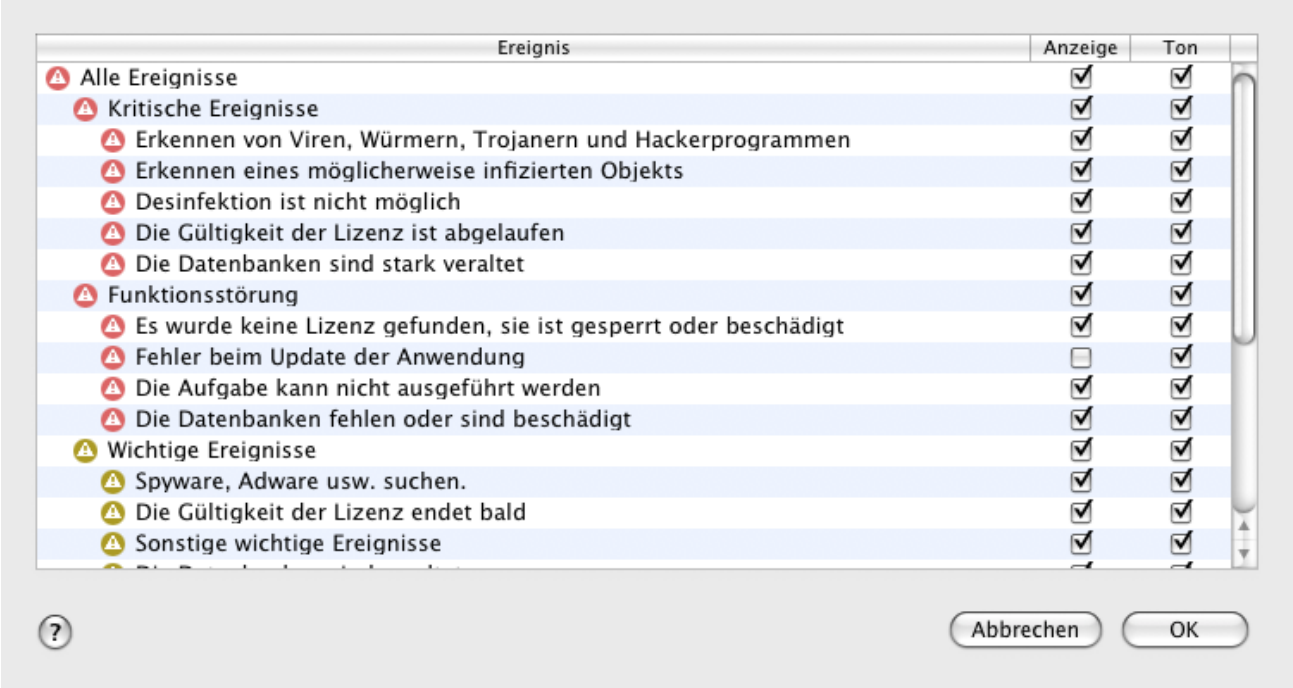

Abbildung 10. Benachrichtigungen konfigurieren

ÜBER POP-UP-MELDUNGEN

Kaspersky Anti-Virus blendet auf dem Bildschirm *Pop-up-Meldungen* ein, um über Ereignisse zu informieren, die nicht unbedingt Ihre Handlungswahl beanspruchen. Pop-up-Meldungen erscheinen unter dem Programmsymbol in der Menüleiste und erlöschen automatisch vom Bildschirm bald nach der Erscheinung.

OBERFLÄCHE VON KASPERSKY ANTI-VIRUS ANPASSEN

Sie können das Aussehen von Kaspersky Anti-Virus verändern, indem Sie unterschiedliche grafische Elemente und Farbschemen erstellen und verwenden. Alle in der Programmoberfläche verwendeten Farben, Schriften, Piktogramme und Texte können verändert werden.

➧ *Um eine grafische Oberfläche einzubinden, gehen Sie folgendermaßen vor:*

1. Öffnen Sie das Programmkonfigurationsfenster (auf Seite 35), und wählen Sie die Registerkarte **Ansicht** aus (siehe Abbildung unten).

2. Klicken Sie im Block **Grafische Oberfläche** auf die Schaltfläche **Wählen**, und wählen Sie im folgenden Standardfenster den Ordner aus, in dem sich die Dateien der grafischen Oberfläche befinden.

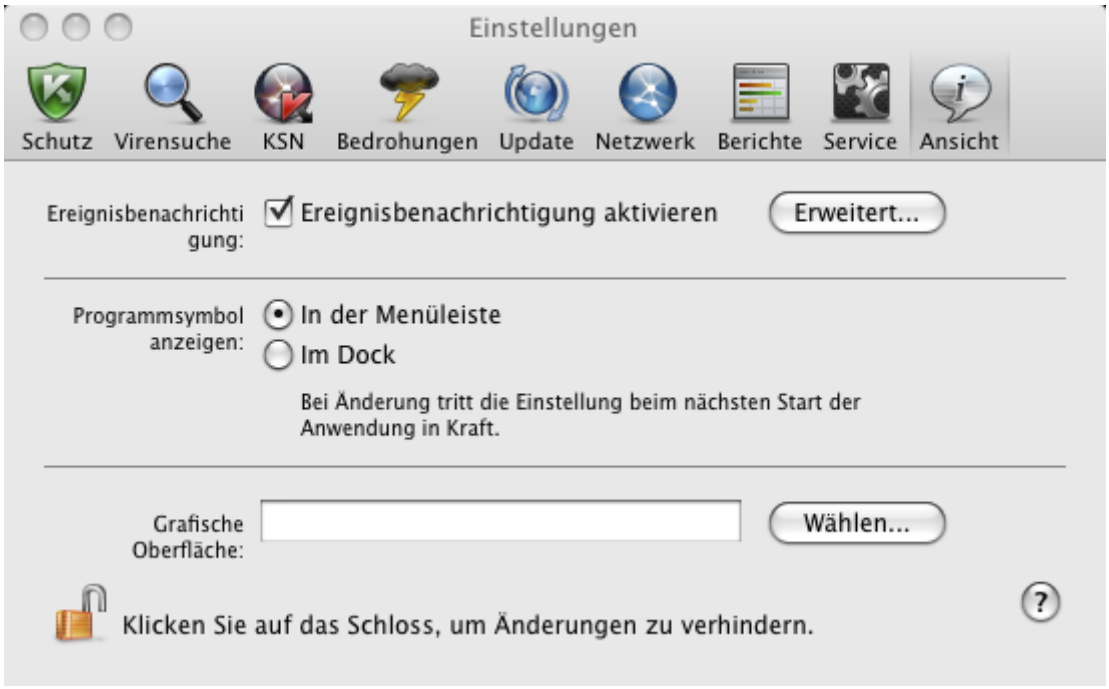

Abbildung 11. Programmkonfigurationsfenster. Ansicht

PROGRAMM STARTEN UND BEENDEN

Dieser Abschnitt informiert darüber, wie das Programm gestartet und beendet wird.

Sofort nach der Installation wird das Programm automatisch gestartet und das Symbol Kaspersky Anti-Virus (auf Seite 32) erscheint in der Menüleiste.

IN DIESEM ABSCHNITT

Kaspersky Anti-Virus beenden 41

Autostart von Kaspersky Anti-Virus anpassen 41

Energiesparmodus anpassen 42

KASPERSKY ANTI-VIRUS BEENDEN

Sollte es aus irgend einer Ursache erforderlich sein, Kaspersky Anti-Virus vollständig zu beenden, klicken Sie auf das Symbol Kaspersky Anti-Virus (siehe Seite 32) in der Menüleiste oder im Dock, und wählen Sie im folgenden Menü den Befehl **Beenden** aus. Das Programm wird beendet, und der Vorgang wird aus dem Arbeitsspeicher des Computers gelöscht.

Nach dem Beenden der Arbeit mit Kaspersky Anti-Virus arbeitet der Computer im ungeschützten Modus weiter und kann einem Infektionsrisiko ausgesetzt werden.

AUTOSTART VON KASPERSKY ANTI-VIRUS ANPASSEN

Standardmäßig wird Kaspersky Anti-Virus automatisch beim Hochfahren des Computers oder nach dem Neustart des Betriebssystems gestartet.

➡ *Um den Autostartmodus zu aktivieren, gehen Sie folgendermaßen vor:*

1. Öffnen Sie das Programmkonfigurationsfenster (siehe Seite 35), wählen Sie die Registerkarte **Service** (siehe Abbildung unten) aus.

2. Deaktivieren Sie im Block **Automatischer Start** das Kontrollkästchen **Programm beim Hochfahren des Computers starten**.

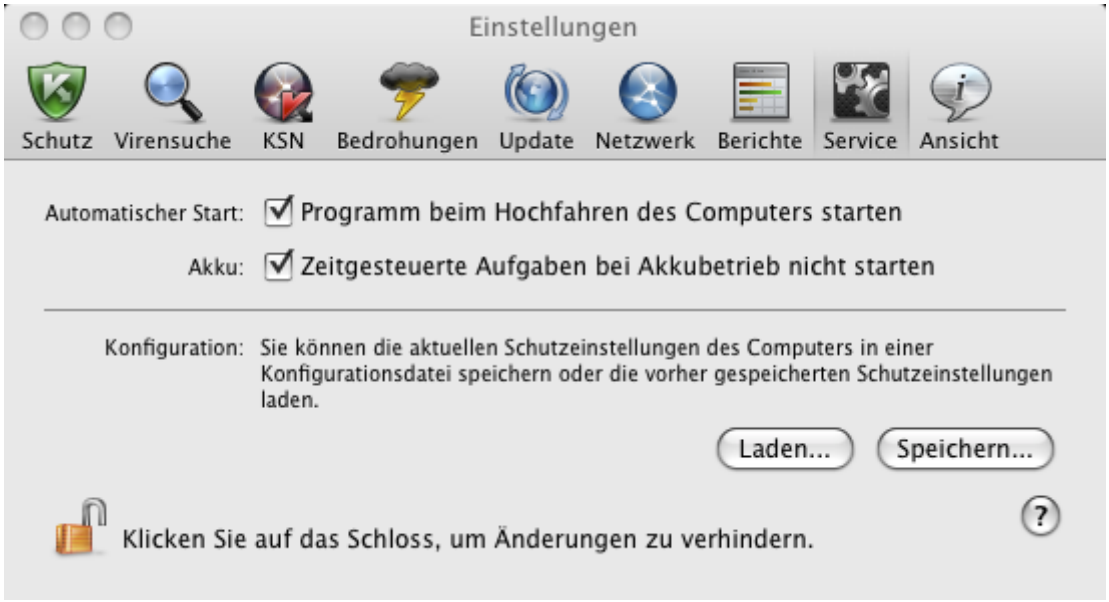

Abbildung 12. Programmkonfigurationsfenster. Service

Die Ausschaltung des Autostartmodus von Kaspersky Anti-Virus führt dazu, dass beim nächsten Neustart des Computers oder des Betriebssystems der Computer im ungeschützten Modus weiter arbeitet und einem Infektionsrisiko ausgesetzt werden kann.

ENERGIESPARMODUS ANPASSEN

Standardmäßig arbeitet Kaspersky Anti-Virus im Energiesparmodus. In diesem Modus werden die Aufgaben zur Virensuche, für die ein Startzeitplan festgelegt ist, nicht gestartet, wenn der Computer im Akkubetrieb arbeitet.

➧ *Um den Energiesparmodus zu deaktivieren, gehen Sie folgendermaßen vor:*

1. Öffnen Sie das Programmkonfigurationsfenster (siehe Seite 35), und wählen Sie die Registerkarte **Service** (siehe Abbildung unten) aus.

2. Deaktivieren Sie im Block **Akku** das Kontrollkästchen **Zeitgesteuerte Aufgaben bei Akkubetrieb nicht starten**.

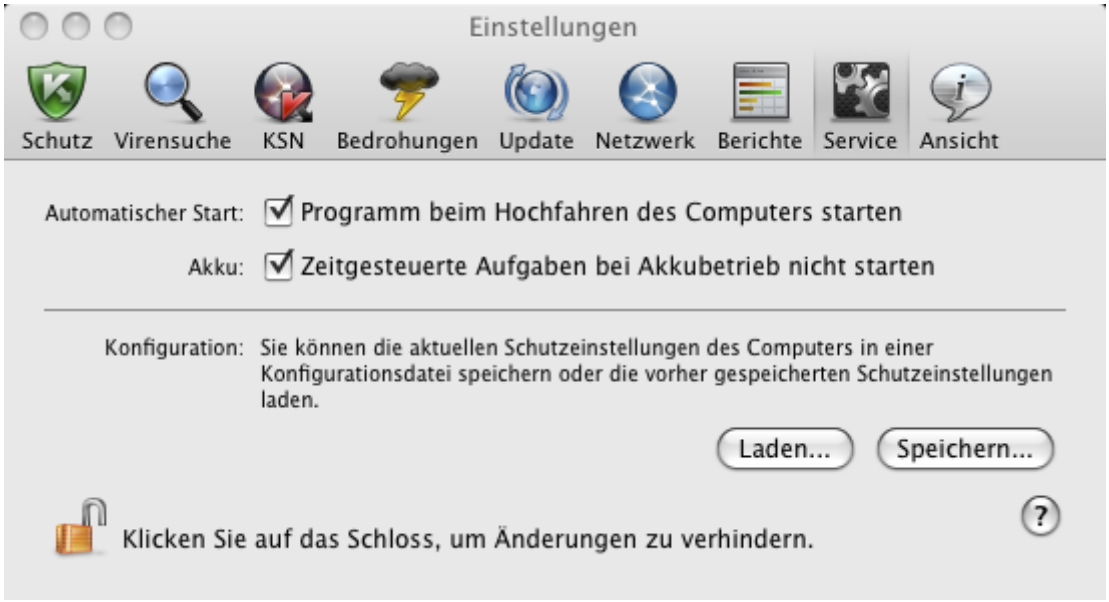

Abbildung 13. Programmkonfigurationsfenster. Service

SCHUTZSTATUS DES COMPUTERS

Der Schutzstatus Ihres Computers informiert anschaulich darüber, ob momentan Bedrohungen vorhanden sind, die das allgemeine Sicherheitsniveau des Systems beeinflussen. Zu Bedrohungen zählen in diesem Fall nicht nur gefundene schädliche Programme, sondern auch die Verwendung von veralteten Antiviren-Datenbanken, Deaktivierung von Datei-Anti-Virus und die Verwendung von Minimaleinstellungen für Kaspersky Anti-Virus.

Der Sicherheitsassistent unterstützt Sie dabei, zuerst die vorhandenen Bedrohungen zu prüfen und sie anschließend zu beseitigen.

IN DIESEM ABSCHNITT

Schutzstatus des Computers einschätzen 44

Sicherheitsassistent 45

SCHUTZSTATUS DES COMPUTERS EINSCHÄTZEN

Der Schutzstatus des Computers wird im Programmhauptfenster (siehe Abschnitt "Programmhauptfenster" auf Seite 34) als Farbindikator angezeigt. Die Farben entsprechen den Signalen einer Verkehrsampel. Abhängig von der Situation verändert sich die Farbe des Indikators. Wenn das Schutzsystem Bedrohungen aufweist, wird der Farbindikator um einen Informationstext erweitert.

Der Schutzstatus kann durch eine der folgenden Farben signalisiert werden:

- **Grün**: Der Schutz Ihres Computers wird auf dem erforderlichen Niveau gewährleistet.

  Dies bedeutet, dass die Antiviren-Datenbanken rechtzeitig aktualisiert wurden, dass Datei-Anti-Virus aktiviert ist, dass Kaspersky Anti-Virus mit den von Kaspersky Lab empfohlenen Einstellungen arbeitet und dass bei der Ausführung von Untersuchungsaufgaben keine schädlichen Objekte gefunden oder die gefundenen schädlichen Objekte neutralisiert wurden.

- **Gelb**: Das Sicherheitsniveau Ihres Computers liegt unter dem Niveau des zuvor beschriebenen Status.

  Dieser Schutzstatus weist darauf hin, dass bei der Arbeit oder in den Einstellungen von Kaspersky Anti-Virus Probleme vorliegen. Dieser Status tritt beispielsweise ein, wenn geringfügige Abweichungen vom empfohlenen Funktionsmodus bestehen oder die Datenbanken von Kaspersky Anti-Virus seit mehreren Tagen nicht mehr aktualisiert wurden.

- **Rot**: Für Ihren Computer besteht ein Infektionsrisiko.

  Dieser Status signalisiert, dass Probleme vorliegen, die zu einer Infektion Ihres Computers und zu Datenverlust führen können. Das ist beispielsweise der Fall, wenn bei der Arbeit von Datei-Anti-Virus eine Störung aufgetreten ist, Kaspersky Anti-Virus sehr lange nicht mehr aktualisiert wurde, schädliche Objekte gefunden wurden, die dringend neutralisiert werden müssen, oder die Anwendung noch nicht aktiviert wurde.

Wenn das Schutzsystem Probleme aufweist, sollten diese umgehend behoben werden. Klicken Sie dazu auf den farbigen Indikator des Hauptfensters, um den Sicherheitsassistenten zu starten (auf Seite 45).

SICHERHEITSASSISTENT

Sicherheitsassistent ist ein Dienst, durch den die vorhandenen Bedrohungen analysiert und sofort beseitigt werden können (siehe Abbildung unten).

➧ *Um den Sicherheitsassistent zu starten,*

klicken Sie auf die Farbanzeige im Programmhauptfenster (siehe Abschnitt "Programmhauptfenster" auf Seite 34).

Die Datenbanken sind veraltet
Die Datenbanken, die von der Anwendung zum Schutz Ihres Computers verwendet werden, sind veraltet. Das bedeutet, dass der Schutz Ihrer Daten nicht dem erforderlichen Niveau entspricht. Es wird empfohlen, die Programm-Datenbanken möglichst bald zu aktualisieren.
Datenbanken aktualisieren
?
Abbrechen
Aufschieben
Zurück
Fortfahren

Abbildung 14. Sicherheitsassistentenoberfläche

Um eine Liste der vorhandenen Bedrohungen anzuzeigen, verwenden Sie die Schaltflächen **Fortfahren** und **Zurück**. Für jede Bedrohung ist eine ausführliche Beschreibung vorhanden und werden folgende Aktionen vorgeschlagen:

- **Bedrohung sofort neutralisieren**.

  Zur Beseitigung der Bedrohung, klicken Sie auf die Schaltfläche mit der Angabe der empfohlenen Aktion. Wenn beispielsweise auf Ihrem Computer infizierte Objekte erkannt worden sind, wird die Aktion **Infizierte Objekte desinfizieren** empfohlen. Wenn die Antiviren-Datenbanken veraltet sind, wird die Aktion **Datenbanken aktualisieren** empfohlen. Ausführliche Informationen zu einer Bedrohung können Sie dem Berichtsfenster entnehmen (siehe Abschnitt "Berichte" auf Seite 98).

- **Neutralisierung der Bedrohung aufschieben**.

  Wenn Sie eine Bedrohung aus irgendeinem Grund nicht sofort beseitigen wollen, schieben Sie diese Aktion auf und führen sie zu einem späteren Zeitpunkt aus. Verwenden Sie dazu die Schaltfläche **Aufschieben**. Beachten Sie, dass diese Möglichkeit nicht für solche ernsthaften Bedrohungen vorgesehen ist, wie zum Beispiel das Vorhandensein von unbearbeiteten schädlichen Objekten, die Störung bei der Arbeit von Datei-Anti-Virus und die Beschädigung von Dateien aus den Datenbanken von Kaspersky Anti-Virus.

Wenn Sie den Sicherheitsassistenten beenden, ohne ernsthafte Bedrohungen entfernt zu haben, wird die Farbe des Indikators im Programmhauptfenster weiter auf Sicherheitsprobleme hinweisen. Die Bedrohungen, deren Neutralisierung Sie aufgeschoben haben, werden beim wiederholten Öffnen des Sicherheitsassistenten nicht in der Liste der aktiven Bedrohungen angezeigt. Zur Liste der aufgeschobenen Bedrohungen und zu deren Neutralisierung können Sie im letzten Fenster des Sicherheitsassistenten durch Klicken auf die Schaltfläche **Aufgeschobene Bedrohungen anzeigen** zurückkehren.

LÖSUNGEN FÜR TYPISCHE AUFGABEN

Dieser Abschnitt beschreibt Aufgaben, die sich den meisten Benutzern bei der Arbeit mit dem Programm stellen, und bietet eine Anleitung zur Ausführung dieser Aufgaben.

IN DIESEM ABSCHNITT

Wie eine vollständige Virenuntersuchung des Computers ausgeführt wird 46

Computer schnell untersuchen 47

Dateien, Ordner und Laufwerke auf Viren untersuchen 47

Wie man eine Suche des Computers nach Zeitplan anpasst 47

Wie eine Lizenz erworben und verlängert wird 48

Wie man die Datenbanken und Programm-Module aktualisiert 48

Wie Programmeinstellungen von Kaspersky Anti-Virus auf einen anderen Computer übertragen werden 49

Empfohlene Aktionen bei blockiertem Zugriff auf eine Datei 49

Was tun, wenn Sie vermuten, dass ein Objekt von einem Virus infiziert ist? 50

Wie ein Objekt wiederhergestellt wird, das vom Programm gelöscht oder desinfiziert wurde 51

Wie man in einen Bericht über die Programmarbeit einsieht 51

Was tun, wenn das Programm Meldungen anzeigt? 51

WIE EINE VOLLSTÄNDIGE VIRENUNTERSUCHUNG DES COMPUTERS AUSGEFÜHRT WIRD

Zum Programm Kaspersky Anti-Virus gehört eine Standardaufgabe zur vollständigen Untersuchung des Computers. Bei der Ausführung dieser Aufgabe untersucht das Programm alle Festplatten auf Viren.

Um die Aufgabe zur vollständigen Untersuchung des Computers zu starten, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Programmhauptfenster (siehe Seite 34), und klicken Sie auf die Schaltfläche .
2. Wählen Sie im folgenden Menü die Aufgabe **Vollständige Suche** aus.

Die Ergebnisse der Aufgabenausführung können Sie im Berichtsfenster anzeigen (siehe Abschnitt "Statistik über die Virensuche" auf Seite 81).

COMPUTER SCHNELL UNTERSUCHEN

Zum Programm Kaspersky Anti-Virus gehört eine Standardaufgabe zur schnellen Untersuchung des Computers. Wenn diese Funktion ausgeführt wird, untersucht das Programm kritische Bereiche des Computers auf Viren: Ordner, die Dateien des Betriebssystems enthalten und Systembibliotheken, deren Schädigung durch schädliche Programme zur Störung des Betriebssystems Ihres Computers führen kann.

Um die Aufgabe zur schnellen Untersuchung des Computers zu starten, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Programmhauptfenster (siehe Seite 34), und klicken Sie auf die Schaltfläche .
2. Wählen Sie im folgenden Menü die Aufgabe **Schnelle Suche** aus.

Die Ergebnisse der Aufgabenausführung können Sie im Berichtsfenster anzeigen (siehe Abschnitt "Statistik über die Virensuche" auf Seite 81).

DATEIEN, ORDNER UND LAUFWERKE AUF VIREN UNTERSUCHEN

Wenn Sie die Virenprüfung eines einzelnen Objekts benötigen (eine der Festplatten, ein einzelner Ordner oder eine Datei, sowie eine Wechselplatte), verwenden Sie die installierte Funktion **Virensuche**.

Um ein einzelnes Objekt auf Viren zu untersuchen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Programmhauptfenster (siehe Seite 34), und klicken Sie auf die Schaltfläche .
2. Wählen Sie im folgenden Menü die Aufgabe **Virensuche** aus. Daraufhin wird das Fenster zur Auswahl von Untersuchungsobjekten geöffnet.
3. Erstellen Sie eine Liste mit Untersuchungsobjekten (siehe Abschnitt "Liste der Untersuchungsobjekte erstellen" auf Seite 72), und klicken Sie auf die Schaltfläche **Start**, um die Aufgabe zur Virensuche zu starten.

Die Ergebnisse der Aufgabenausführung können Sie im Berichtsfenster anzeigen (siehe Abschnitt "Statistik über die Virensuche" auf Seite 81).

Die Virenprüfung eines beliebigen Objekts auf Ihrem Computer kann man aus dem Programm Finder starten, wenn die Komponente **Finder Kontextmenü** installiert wurde (siehe Abschnitt "**Benutzerdefinierte Installation von Kaspersky Anti-Virus**" auf Seite 23). Öffnen Sie dafür das Kontextmenü des Objekts und wählen Sie den Befehl **Auf Viren untersuchen**[1] aus.

WIE MAN EINE SUCHE DES COMPUTERS NACH ZEITPLAN ANPASST

Eine Voraussetzung für die Sicherheit Ihres Computers besteht darin, den Computer rechtzeitig auf Viren zu untersuchen. Sie können einen Zeitplan für den Start der Untersuchungsaufgaben **Schnelle Suche** und **Vollständige Suche** erstellen. In Abhängigkeit von dem ausgewählten Modus wird das Programm automatisch eine Aufgabe starten und den gesamten Computer oder die kritischsten Bereiche des Dateisystems untersuchen.

[1] In den älteren Versionen des Betriebssystems Mac OS X als 10.6 kann sich das Starten des Untersuchungsvorgangs unterscheiden.

- *Um einen Zeitplan für Tasks zur **Schnelle Suche** oder **Vollständige Suche** einzurichten gehen Sie folgendermaßen vor:*

  1. Öffnen Sie das Programmkonfigurationsfenster (siehe Seite 35), und wählen Sie die Registerkarte **Virensuche** aus.

  2. Wählen Sie in der linken Liste die gewünschte Aufgabe aus und aktivieren Sie im Block **Startmodus** den Aufgabenstart nach Zeitplan. Um den Zeitplan für den Aufgabenstart zu ändern, klicken Sie auf die Schaltfläche **Ändern**.

  3. Legen Sie im folgenden Fenster fest, wie oft die Aufgabe zur Virensuche gestartet werden soll.

Die Ergebnisse der Aufgabenausführung können Sie im Berichtsfenster anzeigen (siehe Abschnitt "Statistik über die Virensuche" auf Seite 81).

WIE EINE LIZENZ ERWORBEN UND VERLÄNGERT WIRD

Wenn Sie Kaspersky Anti-Virus installiert haben und keine Lizenz besitzen, können Sie die Lizenz nach der Programminstallation erwerben. Wenn die Gültigkeit der vorhandenen Lizenz bald abläuft, können Sie diese verlängern. Beim Kauf einer Lizenz bzw. Verlängern ihrer Gültigkeitsdauer erhalten Sie einen Aktivierungscode, mit dem das Programm aktiviert wird (siehe Abschnitt "Kaspersky Anti-Virus aktivieren" auf Seite 29).

- *Gehen Sie folgendermaßen vor, um eine Lizenz zu erwerben:*

  1. Öffnen Sie das Programmhauptfenster (siehe Seite 34), und klicken Sie auf die Schaltfläche .

  2. Klicken Sie im folgenden Fenster auf die Schaltfläche **Kaufen**.

     Die Webseite des Online-Shops wird geöffnet. Dort können Sie eine Lizenz erwerben.

- *Gehen Sie folgendermaßen vor, um die Gültigkeitsdauer einer Lizenz zu verlängern:*

  1. Öffnen Sie das Programmhauptfenster (siehe Seite 34), und klicken Sie auf die Schaltfläche .

  2. Klicken Sie im folgenden Fenster auf die Schaltfläche **Verlängern**.

     Daraufhin wird die Webseite des Internet-Shops geöffnet, wo Sie die Gültigkeitsdauer der Lizenz verlängern können.

WIE MAN DIE DATENBANKEN UND PROGRAMM-MODULE AKTUALISIERT

Kaspersky Lab aktualisiert die Datenbanken und Programm-Module von Kaspersky Anti-Virus und veröffentlicht die Updates auf speziellen Updateservern. *Kaspersky-Lab-Updateserver* sind Internetseiten von Kaspersky Lab, auf denen Updates für Kaspersky Anti-Virus regelmäßig zur Verfügung gestellt werden.

Um die Updates von den Servern herunterzuladen, ist eine Verbindung Ihres Computers mit dem Internet erforderlich.

Kaspersky Anti-Virus überprüft in der Grundeinstellung regelmäßig, ob auf den Kaspersky-Lab-Servern neue Updates vorhanden sind. Wenn neue Updates vorhanden sind, lädt sie Kaspersky Anti-Virus im Hintergrund herunter und installiert sie auf dem Computer.

- *Um Kaspersky Anti-Virus manuell zu aktualisieren,*

  öffnen Sie das Programmhauptfenster (siehe Seite 34), und klicken Sie auf die Schaltfläche .

Die Ergebnisse der Aufgabenausführung können Sie im Berichtsfenster anzeigen (siehe Abschnitt "Statistik für das Update" auf Seite 91).

WIE PROGRAMMEINSTELLUNGEN VON KASPERSKY ANTI-VIRUS AUF EINEN ANDEREN COMPUTER ÜBERTRAGEN WERDEN

Kaspersky Anti-Virus bietet Ihnen die Möglichkeit zum Exportieren und Importieren der Programmeinstellungen. Diese Option kann beispielsweise von Nutzen sein, wenn Sie das Programm sowohl auf Ihrem PC zuhause, als auch im Büro installiert haben. Sie können das Programm zu Hause entsprechend Ihrem Arbeitsplan konfigurieren, diese Einstellungen auf einem Datenträger sichern und sie auf Ihren Computer im Büro importieren. Die Einstellungen werden in einer speziellen Konfigurationsdatei gespeichert.

- *Um die aktuellen Einstellungen für Kaspersky Anti-Virus in einer Datei zu sichern, gehen Sie folgendermaßen vor:*

  1. Öffnen Sie das Programmkonfigurationsfenster (auf Seite 35), und wählen Sie die Registerkarte **Service** aus.
  2. Klicken Sie im Block **Konfiguration** auf die Schaltfläche **Sichern**. Daraufhin wird das Fenster **Sichern** geöffnet.
  3. Geben Sie im Feld **Sichern unter** den Dateinamen ein, und wählen Sie den Ordner aus, in dem die Datei gespeichert werden soll.

- *Um die Einstellungen für Kaspersky Anti-Virus aus einer Konfigurationsdatei zu importieren, gehen Sie folgendermaßen vor:*

  1. Das Programmkonfigurationsfenster (siehe Seite 35), und wählen Sie die Registerkarte **Service** aus.
  2. Klicken Sie im Block **Konfiguration** auf die Schaltfläche **Laden**, und wählen Sie im folgenden Standardfenster die Datei mit den Einstellungen für Kaspersky Anti-Virus aus.

EMPFOHLENE AKTIONEN BEI BLOCKIERTEM ZUGRIFF AUF EINE DATEI

Kaspersky Anti-Virus blockiert den Zugang zur Datei oder zum Programm, wenn Datei-Anti-Virus (siehe Seite 56) vermutet, dass das angefragte Objekt infiziert oder möglicherweise mit einem schädlichen Programm infiziert ist, und die Aktion **Zugriff verweigern** ausgewählt ist.

- *Um gefährliche Objekte zu bearbeiten, die auf der Registerkarte **Gefunden** des Berichtsfensters aufgeführt sind, gehen Sie folgendermaßen vor:*

  1. Öffnen Sie das Programmhauptfenster (siehe Seite 34), und klicken Sie auf die Schaltfläche . Daraufhin wird das Berichtsfenster von Kaspersky Anti-Virus geöffnet.
  2. Wählen Sie im linken Bereich des Berichtsfensters **Gefunden** aus. Im rechten Bereich des Fensters wird eine Liste mit gefundenen gefährlichen Objekten mit Statusangabe angezeigt.
  3. Klicken Sie auf die Schaltfläche **Alle desinfizieren**. Bei der Verarbeitung jedes Objekts erscheint auf dem Bildschirm eine Benachrichtigung, die vorschlägt, wie mit dem Objekt künftig verfahren werden soll. Wenn Sie im Meldungsfenster das Kontrollkästchen **In allen ähnlichen Fällen anwenden** aktivieren, wird die ausgewählte Aktion auf alle Objekte mit dem gleichen Status angewendet.

- *Um die möglicherweise infizierten Objekte zu bearbeiten, die in die Quarantäne verschoben wurden, gehen Sie folgendermaßen vor:*

1. Öffnen Sie das Programmhauptfenster (siehe Seite 34), und klicken Sie auf die Schaltfläche . Daraufhin wird das Berichtsfenster von Kaspersky Anti-Virus geöffnet.

2. Wählen Sie im linken Bereich des Fensters **Quarantäne** aus. Auf der rechten Seite des Fensters wird der Inhalt des Speichers angezeigt.

3. Klicken Sie auf die Schaltfläche **Alle untersuchen**, um alle möglicherweise infizierten Quarantäne-Objekte mit den aktuellen Datenbanken von Kaspersky Anti-Virus zu untersuchen und zu desinfizieren.

4. Klicken Sie auf die Schaltfläche **Wiederherstellen**, um die Dateien in einem vom Benutzer vorgegebenen Ordner oder in dem Ordner, aus dem sie in die Quarantäne verschoben wurden (standardmäßig), wiederherzustellen.

   Es wird empfohlen, nur Objekte mit dem Status *Fehlalarm* wiederherzustellen, weil die Wiederherstellung anderer Objekte zu einer Infektion Ihres Computers führen kann.

5. Klicken Sie auf die Schaltfläche **Löschen** oder **Alle löschen**, um das ausgewählte Objekt aus der Quarantäne zu löschen oder um die Quarantäne vollständig zu löschen.

Wenn Sie sich sicher sind, dass die Objekte, die von Datei-Anti-Virus geblockt werden, sicher sind, schließen Sie diese in die vertrauenswürdige Zone ein, indem Sie eine Ausnahmeregel erstellen (siehe Abschnitt "Vertrauenswürdige Zone anlegen" siehe Seite 53).

WAS TUN, WENN SIE VERMUTEN, DASS EIN OBJEKT VON EINEM VIRUS INFIZIERT IST?

Wenn Sie vermuten, dass ein Objekt infiziert sein könnte, prüfen Sie es auf Viren (siehe Abschnitt "Wie eine Datei, ein Ordner oder ein Laufwerk auf Viren untersucht wird" auf Seite 47).

Wenn Kaspersky Anti-Virus als Ergebnis der Prüfung mitteilt, dass das Objekt nicht infiziert ist, Sie aber das Gegenteil vermuten, verschieben Sie das Objekt in die *Quarantäne*. Objekte, die sich in der Quarantäne befinden, werden in eingepackter Form gespeichert und stellen keine Bedrohung für Ihren Computer dar. Möglicherweise kann die Bedrohung eindeutig bestimmt und desinfiziert werden, nachdem die Datenbanken von Kaspersky Anti-Virus aktualisiert wurden.

- *Um ein Objekt in der Quarantäne zu platzieren, gehen Sie folgendermaßen vor:*

1. Öffnen Sie das Programmhauptfenster (siehe Seite 34), und klicken Sie auf die Schaltfläche . Daraufhin wird das Berichtsfenster von Kaspersky Anti-Virus geöffnet.

2. Wählen Sie im linken Bereich des Fensters **Quarantäne** aus. Auf der rechten Seite des Fensters wird der Inhalt des Speichers angezeigt.

3. Klicken Sie auf die Schaltfläche **Hinzufügen** und wählen Sie im folgenden Standardfenster die benötigte Datei aus. Sie wird mit dem Status *vom Benutzer hinzugefügt* zur Liste hinzugefügt.

WIE EIN OBJEKT WIEDERHERGESTELLT WIRD, DAS VOM PROGRAMM GELÖSCHT ODER DESINFIZIERT WURDE

Es wird davor gewarnt, gelöschte und desinfizierte Objekte wiederherzustellen, wenn dies nicht absolut erforderlich ist, da diese eine Gefahr für Ihren Computer darstellen können.

Manchmal gelingt es nicht bei der Desinfektion von infizierten Objekten ihre Unversehrtheit zu sichern. Wenn ein desinfiziertes Objekt wichtige Informationen enthielt, die aufgrund der Desinfektion vollständig oder teilweise verloren gegangen sind, können Sie versuchen, das ursprüngliche Objekt über seine Sicherungskopie wiederherzustellen.

Gehen Sie folgendermaßen vor, um ein Objekt wiederherzustellen, das vom Programm gelöscht oder verändert wurde:

1. Öffnen Sie das Programmhauptfenster (siehe Seite 34), und klicken Sie auf die Schaltfläche . Daraufhin wird das Berichtsfenster von Kaspersky Anti-Virus geöffnet.

2. Wählen Sie im linken Bereich des Fensters **Backup** aus. Daraufhin wird der Inhalt des Backups in Form einer Liste mit Sicherungskopien der Objekte im rechten Bereich des Fensters angezeigt.

3. Wählen Sie die Sicherungskopie des gewünschten Objekts in der Liste aus, und klicken Sie auf die Schaltfläche **Wiederherstellen**. Bestätigen Sie die Aktion im folgenden Fenster. Das Objekt wird unter dem gleichen Namen am ursprünglichen Speicherort wiederhergestellt, den es vor der Desinfektion und Löschung trug. Wenn sich am ursprünglichen Speicherort ein Objekt mit dem gleichen Namen befindet (Diese Situation ist möglich, wenn ein Objekt wiederhergestellt wird, dessen Kopie bereits vor der Desinfektion angelegt wurde), erscheint eine entsprechende Warnung auf dem Bildschirm. Sie können den Speicherort des wiederherzustellenden Objekts ändern oder es umbenennen.

   Es wird empfohlen, das Objekt sofort nach der Wiederherstellung auf Viren zu untersuchen. Möglicherweise gelingt es, das Objekt mit aktualisierten Datenbanken ohne Datenverlust zu desinfizieren.

WIE MAN IN EINEN BERICHT ÜBER DIE PROGRAMMARBEIT EINSIEHT

Die Informationen zu den Ereignissen, die während der Ausführung von Datei-Anti-Virus (siehe Abschnitt "Datei-Anti-Virus" auf Seite 56), bei der Ausführung von Aufgaben der Virensuche (siehe Abschnitt "Virensuche" auf Seite 68) oder Update-Aufgaben (siehe Abschnitt "Programm-Update" auf Seite 83) eingetreten sind, werden im Berichtsfenster (siehe Abschnitt "Berichte" auf Seite 98) angezeigt.

Um das Berichtsfenster zu öffnen,

öffnen Sie das Programmhauptfenster (siehe Seite 34), und klicken Sie auf die Schaltfläche .

WAS TUN, WENN DAS PROGRAMM MELDUNGEN ANZEIGT?

Programmbenachrichtigungen (siehe Abschnitt "Meldungsfenster und Pop-up-Meldungen" auf Seite 36) in Form von Pop-up-Meldungen informieren über Ereignisse, die im Arbeitsvorgang des Programms geschehen und Ihrer Aufmerksamkeit bedürfen.

Erscheint eine solche Benachrichtigung auf dem Bildschirm, muss eine der vorgegebenen Varianten für die weitere Vorgehensweise ausgewählt werden. Als optimal gilt die von Kaspersky Lab empfohlene Variante.

ERWEITERTE PROGRAMMEINSTELLUNGEN

Dieser Abschnitt informiert ausführlich über die einzelnen Komponenten und beschreibt den jeweiligen Funktionsalgorithmus und die Einstellungen.

IN DIESEM ABSCHNITT

Schutzbereich festlegen 52

Datei-Anti-Virus 56

Virensuche 68

Programm-Update 83

Berichte und Speicher 93

Teilnahme am Kaspersky Security Network 102

SCHUTZBEREICH FESTLEGEN

Der Schutzbereich eines Computers wird mithilfe der folgenden Einstellungen angelegt:

- Liste mit schädlichen Programmen, vor denen Kaspersky Anti-Virus Schutz bietet
- Objekte der vertrauenswürdigen Zone, die vom Schutz ausgeschlossen werden.

IN DIESEM ABSCHNITT

Zu kontrollierende schädliche Programme auswählen 52

Vertrauenswürdige Zone anlegen 53

ZU KONTROLLIERENDE SCHÄDLICHE PROGRAMME AUSWÄHLEN

Das Programm Kaspersky Anti-Virus bietet Ihnen Schutz vor verschiedenen Arten schädlicher Programme. Ohne Berücksichtigung der gesetzten Programmeinstellungen schützt das Programm Ihren Computer immer vor den gefährlicheren Arten von Malware: Viren, trojanische Programme und Hacker-Utilities. Diese Programme können Ihrem Computer ernsthaften Schaden zufügen. Um die Sicherheit des Computers zu erhöhen, können Sie die Liste der erkennbaren Bedrohungen erweitern. Aktivieren Sie dazu die Kontrollkästchen der einzelnen Arten potentiell gefährlicher Programme.

Schädliche und potentiell gefährliche Programme, vor denen Kaspersky Anti-Virus schützt, werden folgenderweise gruppiert:

- **Viren, Würmer, Trojaner und Hackerprogramme**: Diese Gruppe umfasst die meistverbreiteten und gefährlichsten Kategorien schädlicher Programme. Den Schutz vor diesen Bedrohungen gewährleistet das minimal erforderliche Sicherheitsniveau. In Übereinstimmung mit den Empfehlungen von Kaspersky Lab werden schädliche Programme dieser Kategorie immer von Kaspersky Anti-Virus kontrolliert.
- **Spyware und Adware**: Diese Gruppe enthält potentiell gefährliche Software, die den Benutzer behindern oder ihm beträchtlichen Schaden zufügen kann.
- **Dialer**: Diese Gruppe umfasst Programme, die Telefonverbindungen über ein Modem versteckt herstellen (einschließlich Dialer für pornographische Telefondienste).
- **Andere Anwendungen**. Diese Gruppe umfasst Programme, die nicht schädlich oder gefährlich sind, aber unter bestimmten Umständen benutzt werden können, um Ihren Computer zu beschädigen.

Um die Gruppen schädlicher Programme auszuwählen, vor denen Kaspersky Anti-Virus Ihren Computer schützen soll, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Programmkonfigurationsfenster (siehe Seite 35), und wählen Sie die Registerkarte **Bedrohungen** (siehe Abbildung unten) aus.

2. Im Block **Malware-Kategorien** aktivieren Sie das Kontrollkästchen neben den Gruppen der schädlichen Software, deren Schutz Kaspersky Anti-Virus gewährleisten soll.

> Kaspersky Anti-Virus bietet immer Schutz für Ihren Computer vor Viren, Würmern, Trojanern und Hacker-Programmen. Deshalb können Sie das Kontrollkästchen neben dieser Gruppe nicht deaktivieren.

In Abhängigkeit von den ausgewählten Gruppen verwendet Kaspersky Anti-Virus die Antiviren-Datenbanken während der Ausführung von Datei-Anti-Virus (siehe Abschnitt "Datei-Anti-Virus" auf Seite 56) und bei der Virensuche (siehe Abschnitt "Virensuche" auf Seite 68) vollständig oder teilweise.

Wenn alle Gruppen der schädlichen Software ausgewählt sind, gewährleistet Kaspersky Anti-Virus den maximalen vollständigen Schutz des Computers. Wenn Sie nur den Schutz vor Viren, Würmern, Trojanern und Hacker-Programmen ausgewählt haben, werden dabei potentiell gefährliche und andere schädliche Programme, die auf Ihrem Computer installiert werden können und durch ihre Aktionen moralischen oder materiellen Schaden verursachen können, von Kaspersky Anti-Virus nicht kontrolliert.

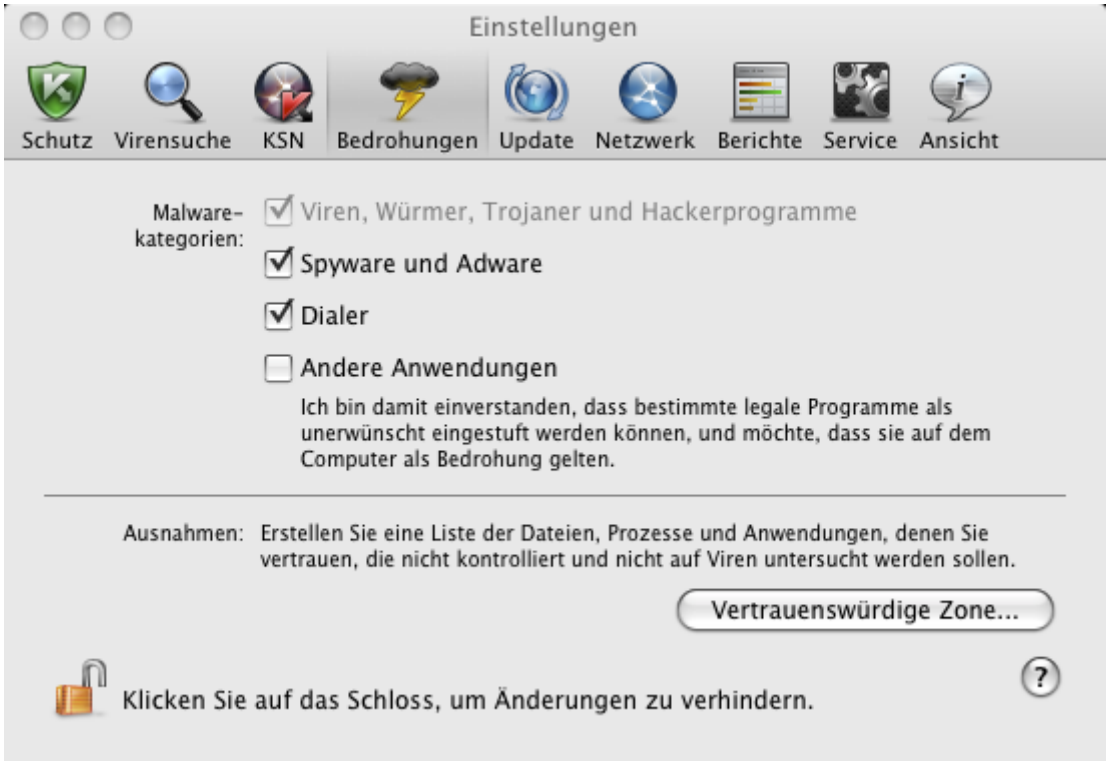

Abbildung 15. Programmkonfigurationsfenster. Bedrohungen

> Die Kaspersky-Lab-Spezialisten warnen davor, die Kontrolle über Spyware, Adware und Dialer zu deaktivieren. Sollte Kaspersky Anti-Virus ein Programm, das Sie für ungefährlich halten, als potentiell gefährlich einstufen, dann wird empfohlen, eine Ausnahmeregel für dieses Programm festzulegen (siehe Abschnitt "Vertrauenswürdige Zone anlegen" auf Seite 53).

VERTRAUENSWÜRDIGE ZONE ANLEGEN

Die *vertrauenswürdige Zone* ist eine benutzerdefinierte Liste von Objekten, die von Kaspersky Anti-Virus nicht kontrolliert werden.

Die vertrauenswürdige Zone wird vom Benutzer abhängig von den Besonderheiten von Objekten, mit denen er arbeitet, sowie von Programmen, die auf seinem Computer installiert sind, aufgebaut. Das Anlegen einer solchen Liste mit Ausnahmen kann beispielsweise erforderlich sein, wenn Kaspersky Anti-Virus den Zugriff auf ein bestimmtes Objekt oder Programm blockiert, Sie aber sicher sind, dass sie für den Computer absolut unschädlich sind.

Eine Ausnahmeregel ist eine Kombination von Bedingungen, bei deren Vorhandensein ein Objekt nicht von Kaspersky Anti-Virus untersucht wird. Von der Untersuchung ausgeschlossen werden können Dateien eines bestimmten Formats (siehe Abschnitt "Liste der Objekte, die auf ihre Erweiterung untersucht werden" auf Seite 115), Dateien mit einem festgelegten Namensschema (siehe Abschnitt "Zulässige Ausschlussmasken für Dateien" auf Seite 117), bestimmte Bereiche (beispielsweise ein Ordner oder Programm) sowie Programmprozesse oder Objekte nach einem Bedrohungstyp gemäß der Klassifikation der Viren-Enzyklopädie (http://www.securelist.com/de).

Ein ausgeschlossenes Objekt unterliegt nicht der Untersuchung, wenn das Laufwerk oder der Ordner untersucht wird, auf dem es sich befindet. Wird allerdings das ausgeschlossene Objekt speziell zur Untersuchung ausgewählt, dann wird die Ausnahmeregel ignoriert.

Ein Bedrohungstyp ist ein Status, der einem Objekt von dem Programm Kaspersky Anti-Virus bei der Untersuchung zugewiesen wird. Der Bedrohungstyp beruht auf einer Klassifikation schädlicher und potentiell gefährlicher Programme, die in der Viren-Enzyklopädie von Kaspersky Lab vorgestellt werden.

Potentiell gefährliche Software besitzt keine schädliche Funktion, kann aber als eine Hilfskomponente eines schädlichen Programms verwendet werden, da sie Lücken und Fehler enthalten kann. Zu dieser Kategorie gehören beispielsweise Programme zur Remote-Verwaltung, IRC-Clients, FTP-Server, alle Hilfsprogramme zum Beenden von Prozessen und zum Verstecken ihrer Arbeit, Tastaturspione, Programme zur Kennwortermittlung, Programme zur automatischen Einwahl auf kostenpflichtige Seiten. Solche Software wird nicht als Virus klassifiziert (not-a-virus), lässt sich aber beispielsweise in folgende Typen unterteilen: Adware, Joke, Riskware u.a. (ausführliche Informationen über potentiell gefährliche Programme, die von Kaspersky Anti-Virus gefunden werden, können Sie unter Viren-Enzyklopädie (http://www.securelist.com/de) einsehen). Derartige Programme können aufgrund der Untersuchung gesperrt werden. Da bestimmte Programme dieser Kategorie von vielen Benutzern verwendet werden, besteht die Möglichkeit, sie von der Untersuchung auszuschließen.

➧ *Um eine neue Ausnahmeregel zu erstellen oder die vorhandenen Ausnahmeregeln anzuzeigen und zu ändern, gehen Sie folgendermaßen vor:*

1. Öffnen Sie das Programmkonfigurationsfenster (auf Seite 35), und wählen Sie die Registerkarte **Bedrohungen** aus (siehe Abbildung unten).

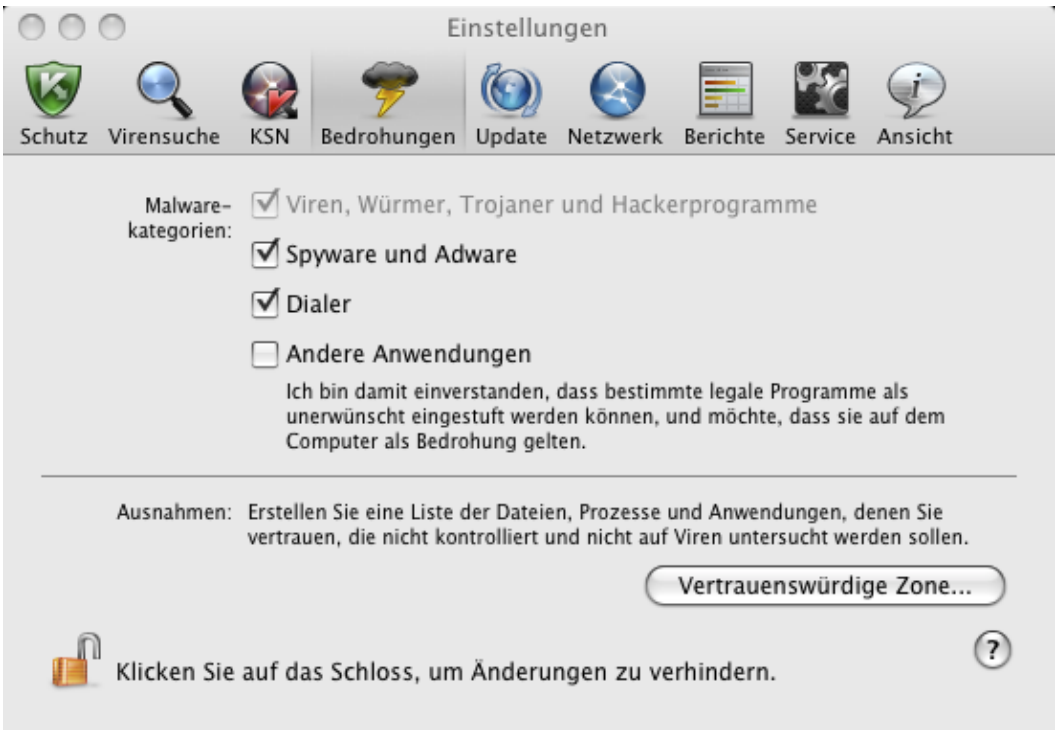

Abbildung 16. Programmkonfigurationsfenster. Bedrohungen

2. Klicken Sie im Block **Ausnahmen** auf die Schaltfläche **Vertrauenswürdige Zone** (siehe Abbildung oben). Ein Fenster mit einer Liste von Objekten wird geöffnet (siehe Abbildung unten), die Kaspersky Anti-Virus nicht im Arbeitsvorgang kontrollieren wird.

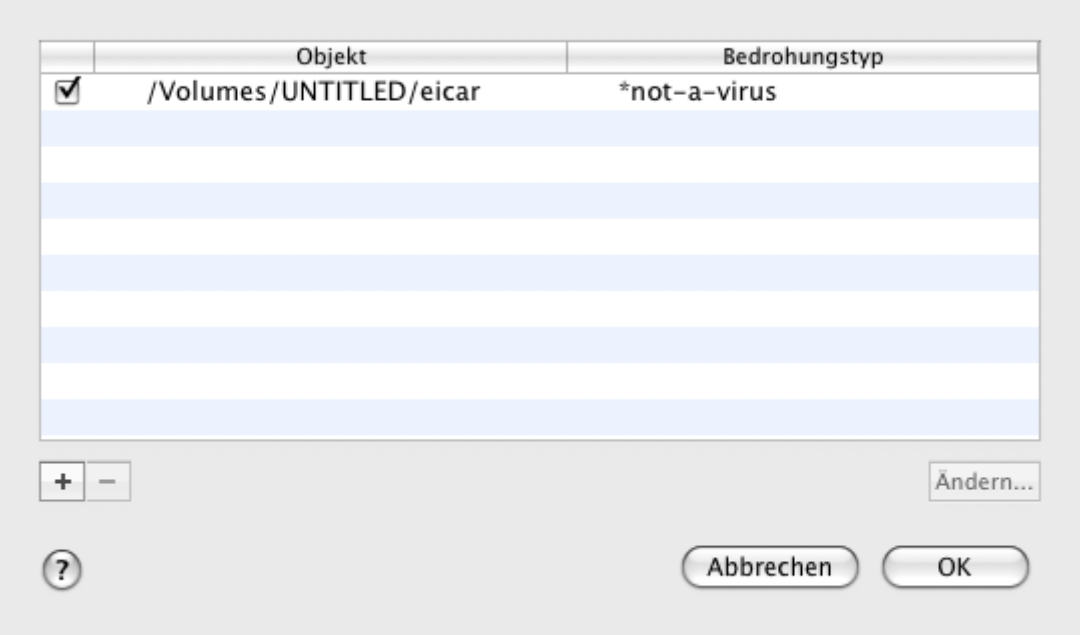

Abbildung 17. Liste der Ausnahmen

Sie können folgende Aktionen ausführen:

- Eine neue Ausnahmeregel erstellen.

  Klicken Sie auf die Schaltfläche +, und legen Sie im folgenden Fenster **Ausnahmeregel** (siehe Abbildung unten) die Bedingungen für die Regel fest.

- Eine erstellte Ausnahmeregel ändern.

  Wählen Sie die gewünschte Ausnahmeregel in der Liste aus, und klicken Sie auf die Schaltfläche **Ändern**. Ändern Sie im folgenden Fenster **Ausnahmeregel** (siehe Abbildung unten) die Bedingungen der Regel.

- Die Verwendung einer Ausnahmeregel vorübergehend deaktivieren.

  Wählen Sie die gewünschte Regel in der Liste aus, und deaktivieren Sie das Kontrollkästchen daneben. Die Ausnahmeregel wird solange nicht angewendet, bis Sie das Kontrollkästchen wieder aktivieren.

- Eine Ausnahmeregel löschen.

  Wählen Sie die gewünschte Ausnahmeregel in der Liste aus, und klicken Sie auf die Schaltfläche −.

Erstellen einer Ausnahmeregel

Legen Sie im folgenden Fenster **Ausnahmeregel** die Bedingungen der Ausnahmeregel entsprechend den folgenden Einstellungen fest:

- **Objekt / Alle Objekte**: Geben Sie eine Datei, einen Ordner oder eine Dateimaske (siehe Abschnitt "Zulässige Ausschlussmasken für Dateien" auf Seite 117) als Ausschlussobjekt an. Sie können den Namen / die Namensmaske des Objekts in das Feld manuell eintragen oder das Objekt im Standardfenster auswählen, das sich durch Klicken auf die Schaltfläche **Wählen** öffnet.

Bei Auswahl von **Alle Objekte** werden alle Objekte Ihres Computers von der Untersuchung ausgeschlossen, die die Bedrohungsart zugewiesen bekommen haben, die im unteren Feld eingegeben wurde.

- **Bedrohungstypen / Alle Bedrohungen**. Mit diesem Parameter werden Objekte von der Untersuchung nach der Bedrohungsart ausgeschlossen, die nach Klassifikation der Virenenzyklopädie zugewiesen wurde. Zur Eingabe des Bedrohungsnamens verwenden Sie die Werte aus der Dropdown-Liste: **beginnen mit**, **enden auf**, **enthalten**, **ganzes Wort** und geben im rechten Feld den entsprechenden Teil der Bezeichnung ein. Beispiel: wenn der Wert **beginnen mit not-a-virus** ausgewählt ist, werden legale, aber potentiell gefährliche Programme aus der Prüfung ausgeschlossen. Außerdem dürfen Bedrohungsnamen mit Platzhaltern (siehe Abschnitt "Zulässige Ausschlussmasken gemäß der Klassifikation der Viren-Enzyklopädie" auf Seite 118) eingegeben werden.

  Bei Auswahl von **Alle Bedrohungen** werden **Objekte** von der Untersuchung ausgeschlossen, die im oben stehenden Feld angegeben wurden, egal, welche Bedrohungsart ihnen zugewiesen wurde.

  Werden gleichzeitig Ausschlussobjekte und Bedrohungsarten ausgewählt, wird die Regel wie folgt angewendet:

  - Wenn als Objekt eine bestimmte Datei festgelegt wird und als Bedrohungstyp ein bestimmter Status, dann wird die angegebene Datei nur dann ausgeschlossen, wenn ihr während der Untersuchung der Status der festgelegten Bedrohung zugewiesen wird.

  - Wenn als Objekt ein bestimmter Bereich oder ein Ordner angegeben wird und als Bedrohungstyp ein bestimmter Status, dann werden nur Objekte des gewählten Status von der Untersuchung ausgeschlossen, die im festgelegten Bereich bzw. Ordner gefunden werden.

- **Komponente / Alle Komponenten**: Wählen Sie die Komponenten von Kaspersky Anti-Virus aus, in deren Arbeit die zu erstellende Regel verwendet werden soll: **Datei-Anti-Virus** oder **Virensuche**.

  Die Variante **Alle Komponenten** bedeutet, dass die Regel für alle Aufgaben der Virensuche sowie für Datei-Anti-Virus verwendet wird.

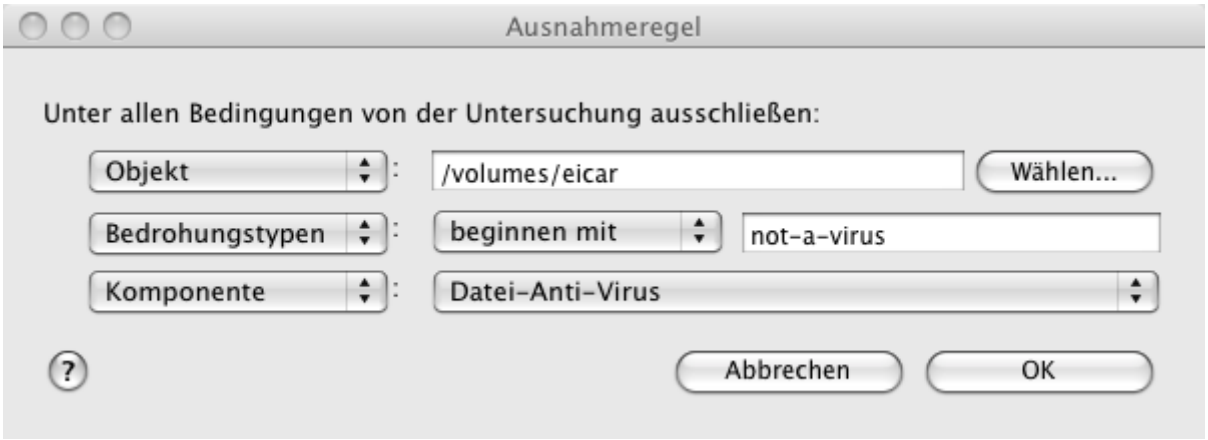

Abbildung 18. Erstellen einer Ausnahmeregel

DATEI-ANTI-VIRUS

Das Dateisystem des Computers kann Viren und andere Schadprogramme enthalten, die jahrelang unbemerkt bleiben, nachdem sie über einen Wechseldatenträger oder das Internet eingedrungen sind.

Datei-Anti-Virus ist eine Komponente, die das Dateisystem des Computers in Echtzeit kontrolliert. Sie wird standardmäßig beim Hochfahren des Betriebssystems gestartet, befindet sich ständig im Arbeitsspeicher des Computers und untersucht alle Dateien, die auf Ihrem Computer und auf den angeschlossenen Laufwerken geöffnet, gespeichert und gestartet werden.

Datei-Anti-Virus untersucht Dateien nach dem folgenden Algorithmus:

1. Die Komponente fängt den Zugriff des Benutzers oder eines Programms auf eine beliebige Datei ab.

2. und überprüft, ob die Informationen über die abgefangene Datei in der iSwift-Datenbank enthalten sind (siehe Abschnitt "Zusätzliche Parameter anpassen" auf Seite 64). Auf Grundlage der erhaltenen Informationen wird über die Notwendigkeit der Untersuchung der Datei entschieden.

3. Datei-Anti-Virus untersucht die Datei auf das Vorhandensein von Viren. Objekte werden auf Grundlage der Datenbanken von Kaspersky Anti-Virus erkannt. Die Datenbanken enthalten eine Beschreibung aller momentan bekannten schädlichen Programme und entsprechende Desinfektionsmethoden.

In Abhängigkeit von den Ergebnissen der Untersuchung bestehen folgende Varianten für das weitere Vorgehen von Kaspersky Anti-Virus:

- Wenn in der Datei kein schädlicher Code gefunden wird, wird der Zugriff darauf sofort freigegeben.

- Wenn in der Datei schädlicher Code gefunden wird, sperrt Datei-Anti-Virus die Datei, speichert eine Kopie im Backup und versucht, die Datei zu desinfizieren. Bei erfolgreicher Desinfektion wird die Datei zum Zugriff freigegeben. Wenn die Desinfektion fehlschlägt, wird die Datei gelöscht. Eine Kopie der Datei wird ins Backup (auf Seite 96) verschoben.

- Wenn in der Datei ein Code entdeckt wird, der einem schädlichen Code ähnelt, wird die Datei in einen speziellen Speicher verschoben – Quarantäne (auf Seite 93). Später kann versucht werden, das Objekt mit aktualisierten Datenbanken zu desinfizieren.

Kaspersky Anti-Virus wird in der Grundeinstellung automatisch beim Start des Betriebssystems gestartet und schützt Ihren Computer während der gesamten Sitzung. Auf die Arbeit von Datei-Anti-Virus weist das Symbol von Kaspersky Anti-Virus (auf Seite 32). Wenn das Symbol aktiv ist, ist der Schutz Ihres Computers aktiviert. Ist das Symbol inaktiv, dann wurde der Schutz deaktiviert.

IN DIESEM ABSCHNITT

Deaktivierung des Dateischutzes 57

Computerschutz fortsetzen 59

Datei-Anti-Virus konfigurieren 60

Standardparameter für den Dateischutz wiederherstellen 66

Statistik über den Dateischutz 66

DEAKTIVIERUNG DES DATEISCHUTZES

Kaspersky Lab empfiehlt ausdrücklich, den Echtzeitschutz nicht zu deaktivieren, weil dies zu einer Infektion Ihres Computers und zu Datenverlust führen kann.

Beachten Sie, dass der Schutz hier ausdrücklich im Kontext von Datei-Anti-Virus beschrieben wird (siehe Abschnitt "Datei-Anti-Virus" auf Seite 56). Wenn Datei-Anti-Virus deaktiviert oder angehalten wird, hat dies keine Auswirkungen auf die Ausführung von Untersuchungs- (siehe Abschnitt "Virensuche" auf Seite 68) und Updateaufgaben (siehe Abschnitt "Programm-Update" auf Seite 83).

Es gibt mehrere Methoden, um Datei-Anti-Virus zu deaktivieren. Bevor der Dateischutz deaktiviert wird, sollten Sie allerdings Ihre Gründe dafür genau abwägen.

Möglicherweise besteht eine andere Möglichkeit. Es kann beispielsweise eine andere Sicherheitsstufe ausgewählt werden (siehe Abschnitt "Sicherheitsstufe auswählen" auf Seite 60) oder der Schutz kann nur für bestimmte Dateien durch Anlegen einer Ausnahmeregel (siehe Abschnitt "Vertrauenswürdige Zone anlegen" auf Seite 53) deaktiviert

werden. Wenn Sie beispielsweise eine bestimmte Datenbank verwenden, von der Sie sicher sind, dass sie virenfrei ist, fügen Sie das Verzeichnis mit ihren Dateien einfach zur vertrauenswürdigen Zone hinzu. Bei Konflikten zwischen Kaspersky Anti-Virus und anderen Programmen auf Ihrem Computer kann es erforderlich sein, Datei-Anti-Virus vorübergehend zu beenden.

Um Datei-Anti-Virus zu deaktivieren, gehen Sie folgendermaßen vor:

- Klicken Sie auf das Symbol von Kaspersky Anti-Virus (auf Seite 32), und wählen Sie im Kontextmenü den Befehl **Schutz deaktivieren** aus (siehe Abbildung unten).

Abbildung 19. Deaktivierung von Datei-Anti-Virus

- Öffnen Sie das Programmkonfigurationsfenster (siehe Seite 35), wählen Sie die Registerkarte **Schutz** aus, und deaktivieren Sie das Kontrollkästchen **Datei-Anti-Virus aktivieren** (siehe Abbildung unten) aus.

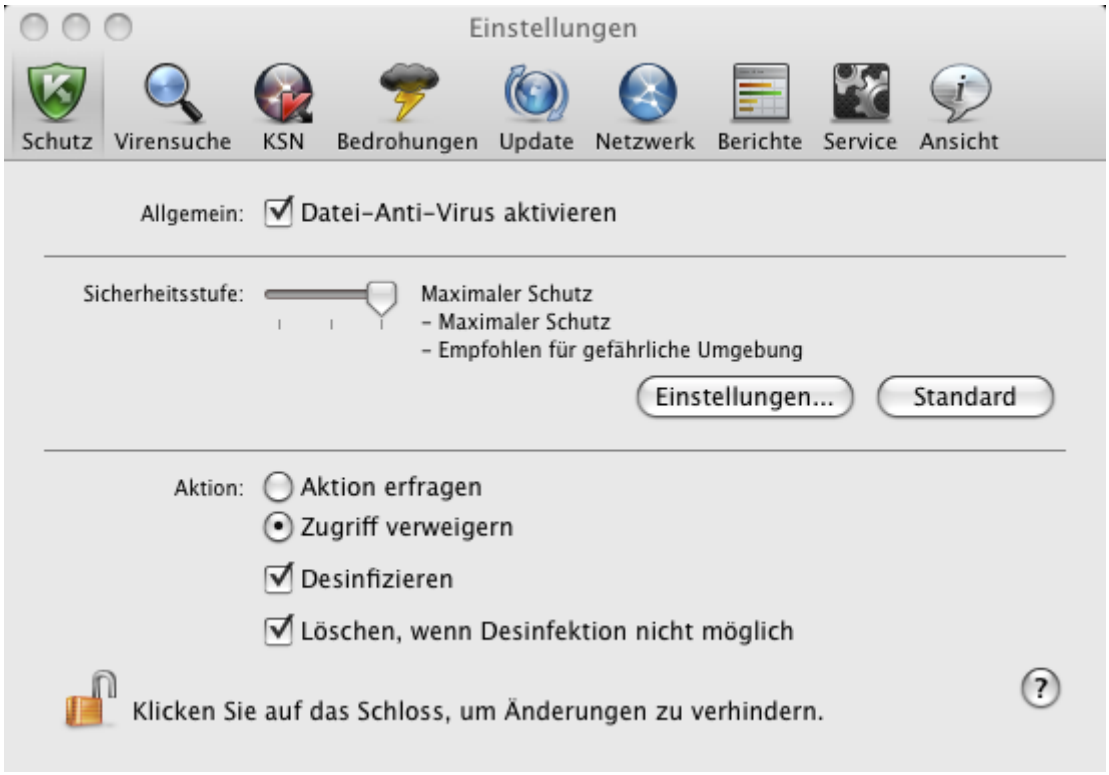

Abbildung 20. Programmkonfigurationsfenster. Schutz

Wenn Sie Datei-Anti-Virus deaktiviert haben, wird die Komponente nach einem Neustart von Kaspersky Anti-Virus nicht automatisch gestartet. Stellen Sie den Schutz des Dateisystems des Computers manuell wieder her (siehe Abschnitt "Computerschutz fortsetzen" auf Seite 59).

COMPUTERSCHUTZ FORTSETZEN

Wenn Datei-Anti-Virus deaktiviert wurde, kann der Schutz des Dateisystems des Computers nur durch den Benutzer manuell wieder aktiviert werden. In diesem Fall wird Datei-Anti-Virus nach einem Neustart des Betriebssystems oder von Kaspersky Anti-Virus nicht automatisch aktiviert.

Um Datei-Anti-Virus zu aktivieren, gehen Sie folgendermaßen vor:

- Klicken Sie auf das Symbol Kaspersky Anti-Virus (auf Seite 32), und wählen Sie im folgenden Kontextmenü den Befehl **Schutz aktivieren** (siehe Abbildung unten) aus.

Abbildung 21. Aktivierung von Datei-Anti-Virus

- Öffnen Sie das Programmkonfigurationsfenster (auf Seite 35), wählen Sie die Registerkarte **Schutz** aus, und aktivieren Sie das Kontrollkästchen **Datei-Anti-Virus Aktivieren**(siehe Abbildung unten).

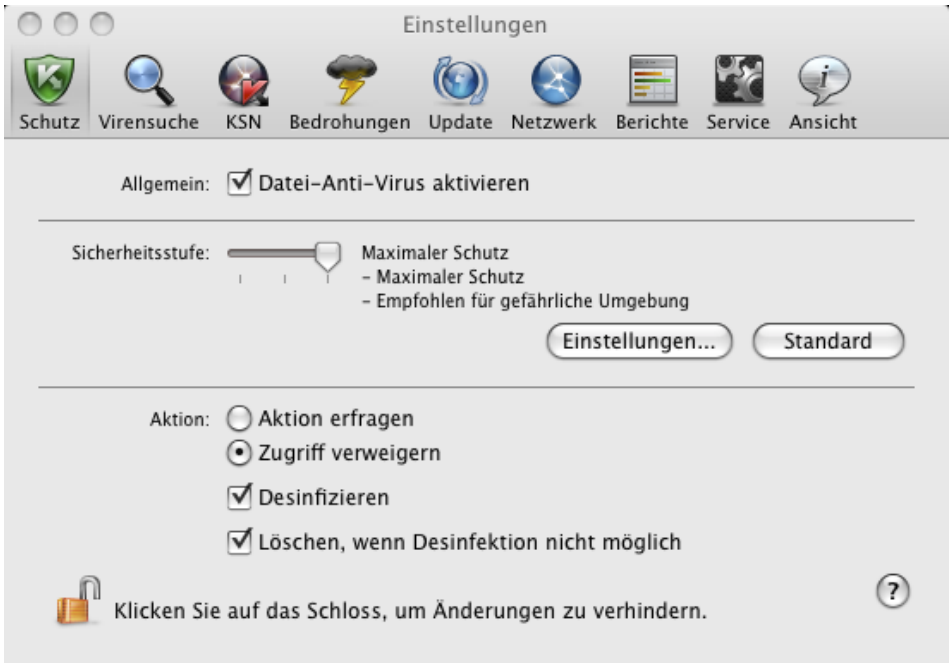

Abbildung 22. Programmkonfigurationsfenster. Schutz

- Verwenden Sie den Sicherheitsassistenten (siehe Abschnitt "Sicherheitsassistent" auf Seite 45). Wenn der Schutz angehalten oder vollständig deaktiviert wird, erhöht sich das Risiko einer Infektion des Computers erheblich. Deshalb wird dieses Risiko sofort vom Sicherheitsassistenten registriert.

DATEI-ANTI-VIRUS KONFIGURIEREN

Datei-Anti-Virus wird mithilfe der folgenden Parameter eingestellt:

- **Sicherheitsstufe**:

  Die Sicherheitsstufe entspricht einer Auswahl von Parametern, die das Verhältnis zwischen der Genauigkeit und der Geschwindigkeit der Objektuntersuchung bestimmen. Drei vordefinierte Sicherheitsstufen (siehe Abschnitt "Sicherheitsstufe auswählen" auf Seite 60) sind verfügbar, deren Einstellungen die Spezialisten von Kaspersky Lab erarbeitet haben.

- **Aktion für ein gefundenes Objekt**:

  Die Aktion (siehe Abschnitt "Aktion für Objekte auswählen" auf Seite 65) bestimmt, wie Kaspersky Anti-Virus beim Fund eines infizierten oder möglicherweise infizierten Objekts reagiert.

SICHERHEITSSTUFE AUSWÄHLEN

Datei-Anti-Virus gewährleistet den Schutz für das Dateisystem des Computers auf einer der folgenden Stufen:

- **Maximaler Schutz**: Auf dieser Stufe erfolgt die Kontrolle über alle Dateien, die geöffnet, gespeichert und gestartet werden, mit maximaler Ausführlichkeit.

- **Empfohlen**: Die Einstellungen dieser Stufe werden von den Kaspersky-Lab-Spezialisten empfohlen.

- **Maximales Tempo**: Diese Stufe erlaubt Ihnen, komfortabel mit Anwendungen zu arbeiten, die den Arbeitsspeicher stark beanspruchen, weil die Auswahl der zu untersuchenden Dateien auf dieser Stufe eingeschränkt wird.

Standardmäßig wird Datei-Anti-Virus auf der Sicherheitsstufe **Empfohlen** ausgeführt. Sie können die Sicherheitsstufe des Dateisystems erhöhen oder senken, indem Sie die Stufe **Maximaler Schutz** oder **Maximales Tempo** auswählen oder die Einstellungen der aktuellen Stufe ändern.

➧ *Gehen Sie folgendermaßen vor, um die festgelegte Sicherheitsstufe zu ändern:*

1. Öffnen Sie das Programmkonfigurationsfenster (siehe Seite 35), und wählen Sie die Registerkarte **Schutz** (siehe Abbildung unten) aus.

2. Verschieben Sie den Schieberegler auf der Skala im Block **Sicherheitsstufe**. Durch das Anpassen der Sicherheitsstufe wird das Verhältnis zwischen der Ausführungsgeschwindigkeit der Untersuchung und der Anzahl der zu untersuchenden Dateien bestimmt: Je weniger Dateien der Virenanalyse unterzogen werden, desto höher ist die Untersuchungsgeschwindigkeit.

Wenn keine der vordefinierten Sicherheitsstufen Ihren Anforderungen entspricht, können Sie die Schutzparameter zusätzlich anpassen. Wählen Sie dazu die Sicherheitsstufe aus, die Ihren Anforderungen am nächsten kommt, und passen Sie ihre Parameter entsprechend an. In diesem Fall ändert sich der Name der Sicherheitsstufe in **Benutzerdefiniert**.

➧ *Um die Einstellungen der aktuellen Sicherheitsstufe anzupassen, gehen Sie folgendermaßen vor:*

1. Öffnen Sie das Programmkonfigurationsfenster (siehe Seite 35), und wählen Sie die Registerkarte **Schutz** (siehe Abbildung unten) aus.

2. Klicken Sie im Block **Sicherheitsstufe** auf die Schaltfläche **Einstellungen**.

3. Passen Sie im folgenden Fenster die Einstellungen für den Dateischutz an:

   - Legen Sie auf der Registerkarte **Allgemein** (siehe Abschnitt "**Typen der zu untersuchenden Dateien festlegen**" auf Seite 61) die Typen der zu untersuchenden Dateien fest.

   - Geben Sie auf der Registerkarte **Schutzbereich** (siehe Abschnitt "**Schutzbereich festlegen**" auf Seite 62) die Laufwerke oder die Ordner an, die von Datei-Anti-Virus kontrolliert werden sollen.

   - Stellen Sie auf der Registerkarte **Erweitert** (siehe Abschnitt "**Zusätzliche Parameter anpassen**" auf Seite 64) den Funktionsmodus für die Komponente ein.

4. Klicken Sie auf die Schaltfläche **OK**, um die Einstellungen zu sichern.

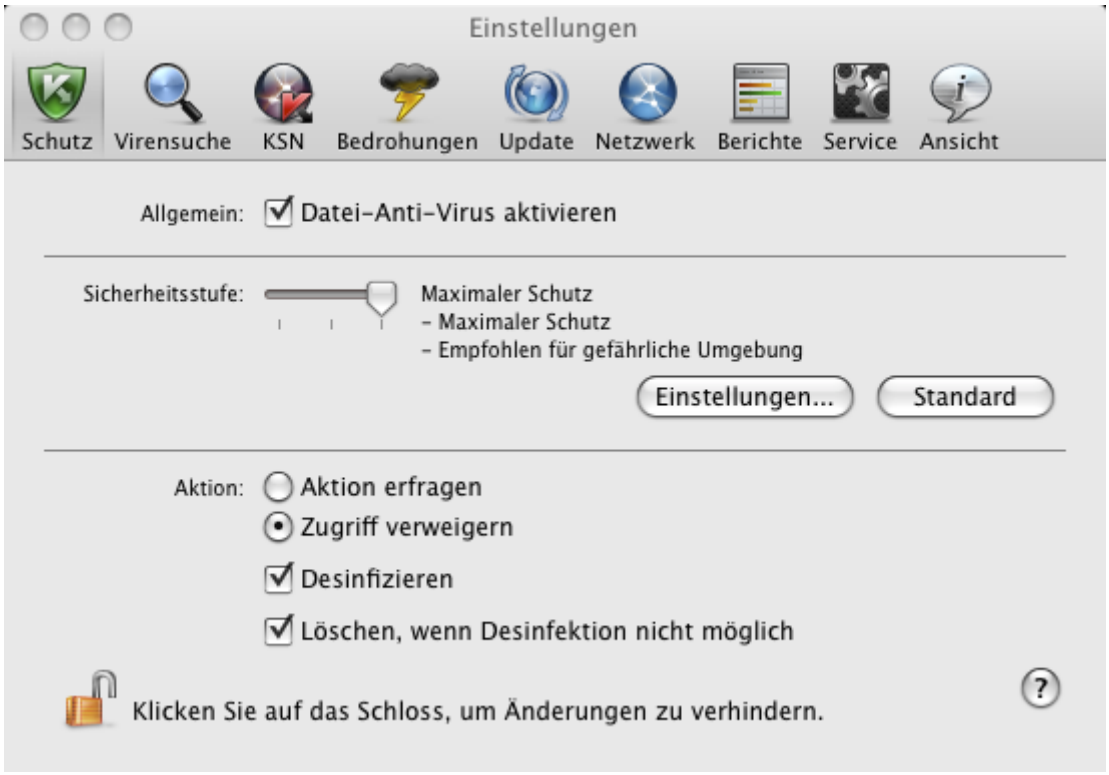

Abbildung 23. Programmkonfigurationsfenster. Schutz

TYPEN DER ZU UNTERSUCHENDEN DATEIEN FESTLEGEN

Durch die Angabe des Typs der zu untersuchenden Dateien definieren Sie das Format und die Größe der Dateien, die beim Öffnen, Ausführen und Sichern von Datei-Anti-Virus untersucht werden sollen. Sie können genauso die Leistungsfähigkeit der Prüfung anpassen.

➧ *Um den Typ der durch Datei-Anti-Virus zu untersuchten Objekte anzugeben und die Leistungsfähigkeit der Prüfung anzupassen, gehen Sie folgendermaßen vor:*

1. Das Programmkonfigurationsfenster (siehe Seite 35), und wählen Sie die Registerkarte **Schutz** aus.

2. Klicken Sie im Block **Sicherheitsstufe** auf die Schaltfläche **Einstellungen**.

3. Wählen Sie im folgenden Fenster die Registerkarte **Allgemein** (siehe Abbildung unten) aus, und passen Sie die folgenden Einstellungen an:

   - Geben Sie im Block **Dateitypen** das Format an, in welchem die Objekte von Kaspersky Anti-Virus beim Öffnen, Ausführen und Sichern auf Viren geprüft werden.
   - Passen Sie im Block **Optimierung** die Leistungsfähigkeit der Prüfung an.
   - Wählen Sie im Block **Zusammengesetzte Dateien** aus, welche zusammengesetzte Dateien unbedingt auf das Vorhandensein von Viren geprüft werden sollen und stellen Sie eine Beschränkung für die Prüfung von großen Objekten fest.

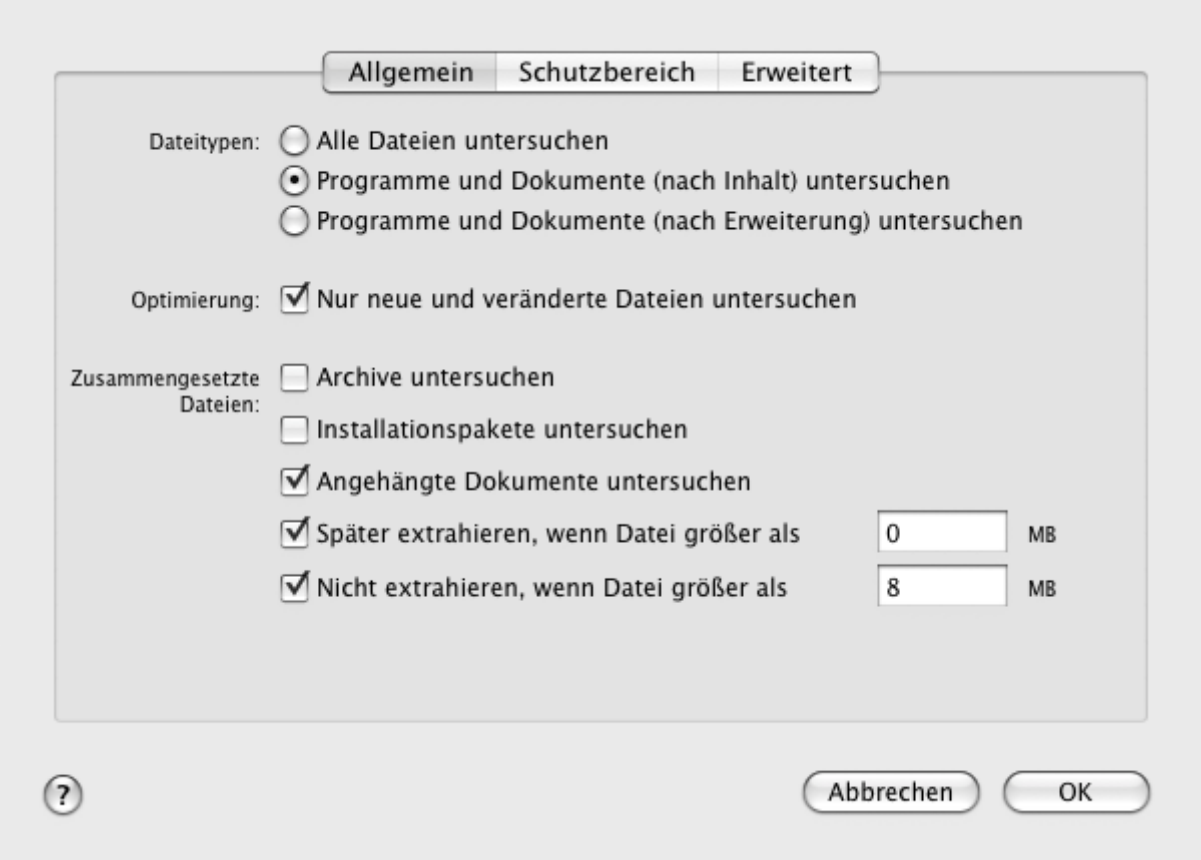

Abbildung 24. Datei-Anti-Virus: Untersuchungsparameter anpassen

SCHUTZBEREICH FESTLEGEN

Datei-Anti-Virus untersucht standardmäßig alle Dateien, auf die zugegriffen wird, und zwar unabhängig davon, auf welchem Datenträger sie sich befinden (Festplatte, CD/DVD-ROM oder USB-Stick).

➧ *Um eine Liste mit den Objekten zu erstellen, die zum Schutzbereich gehören, gehen Sie folgendermaßen vor:*

1. Das Programmkonfigurationsfenster (siehe Seite 35), und wählen Sie die Registerkarte **Schutz** aus.
2. Klicken Sie im Block **Sicherheitsstufe** auf die Schaltfläche **Einstellungen**.
3. Wählen Sie im folgenden Fenster die Registerkarte **Schutzbereich** (siehe Abbildung unten) aus. Auf dieser Registerkarte wird eine Liste der Objekte angezeigt, die von Datei-Anti-Virus untersucht werden sollen. Standardmäßig ist der Schutz für alle Objekte aktiviert, die sich auf Festplatten, Wechseldatenträgern und Netzlaufwerken befinden, die an Ihren Computer angeschlossen sind.

Sie können folgende Aktionen ausführen:

- Objekte für die Untersuchung hinzufügen.

  Klicken Sie auf die Schaltfläche [+], und wählen Sie im folgenden Standardfenster einen Ordner oder eine Datei aus.

- Objekte in der Liste ändern (Dies ist nur für die Objekte verfügbar, die der Benutzer hinzugefügt hat).

  Wählen Sie ein Objekt aus, und klicken Sie auf die Schaltfläche **Ändern**. Nehmen Sie im folgenden Fenster die erforderlichen Änderungen vor.

- Bestimmte Objekte der Liste vorübergehend von der Untersuchung ausschließen.

  Wählen Sie ein Objekt aus, und deaktivieren Sie das entsprechende Kontrollkästchen. Das Objekt wird von Datei-Anti-Virus nicht kontrolliert, bis das Kontrollkästchen wieder aktiviert ist.

- Objekte löschen (Dies ist nur für die Objekte verfügbar, die der Benutzer hinzugefügt hat).

  Wählen Sie ein Objekt aus, und klicken Sie auf die Schaltfläche [−].

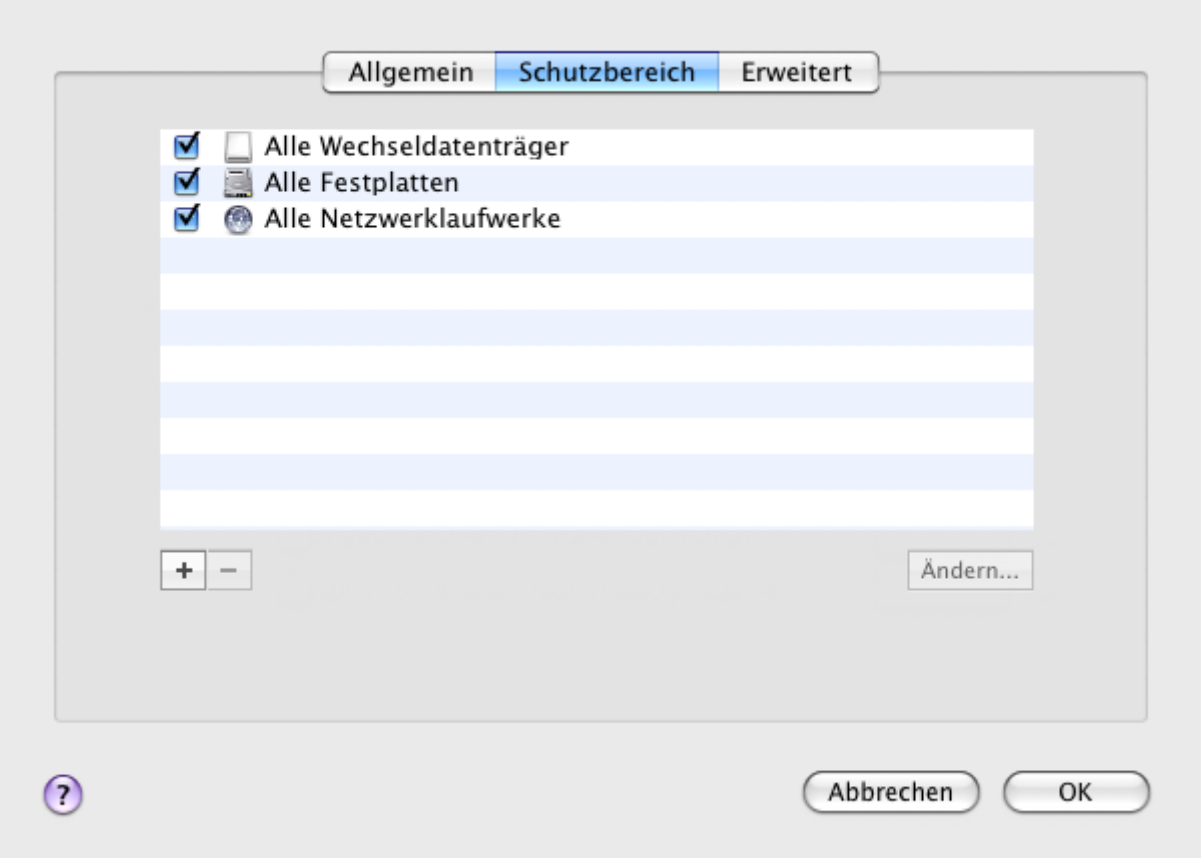

Abbildung 25. Datei-Anti-Virus: Schutzbereich erstellen

Wenn Sie den Bereich der zu schützenden Objekte einschränken möchten, können Sie folgendermaßen vorgehen:

- nur die Ordner, Laufwerke oder Dateien angeben, die geschützt werden sollen;

- eine Liste der Objekte anlegen, die nicht geschützt werden sollen (siehe Abschnitt "Vertrauenswürdige Zone anlegen" auf Seite 53);

- die erste und zweite Methode verbinden, d.h. einen Schutzbereich erstellen, aus dem bestimmte Objekte ausgeschlossen werden.

ZUSÄTZLICHE PARAMETER ANPASSEN

Als zusätzliche Parameter für Datei-Anti-Virus können Sie den Untersuchungsmodus für die Objekte des Dateisystems einstellen, iSwift-Technologie aktivieren, die Leistungsfähigkeit der Objektverarbeitung steigert, und den Zeitplan für die Funktion der Komponente einstellen.

Um die zusätzlichen Parameter von Datei-Anti-Virus anzupassen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Programmkonfigurationsfenster (siehe Seite 35), und wählen Sie die Registerkarte **Schutz** aus.
2. Klicken Sie im Block **Sicherheitsstufe** auf die Schaltfläche **Einstellungen**.
3. Wählen Sie im folgenden Fenster die Registerkarte **Erweitert** (siehe Abbildung unten) aus, und passen Sie die folgenden Einstellungen an:
   - Legen Sie im Block **Untersuchungsmodus** die Einstellungen für das Auslösen von Datei-Anti-Virus fest.
   - Legen Sie im Block **Leistung** die Untersuchungstechnologie fest.
   - Aktivieren Sie im Block **Aufgabe anhalten** das Anhalten der Arbeit von Datei-Anti-Virus nach Zeitplan und passen Sie die Einstellungen des Zeitplans an.
   - Passen Sie im Block **Heuristische Analyse** die Benutzung von Datei-Anti-Virus der heuristischen Analyse an.

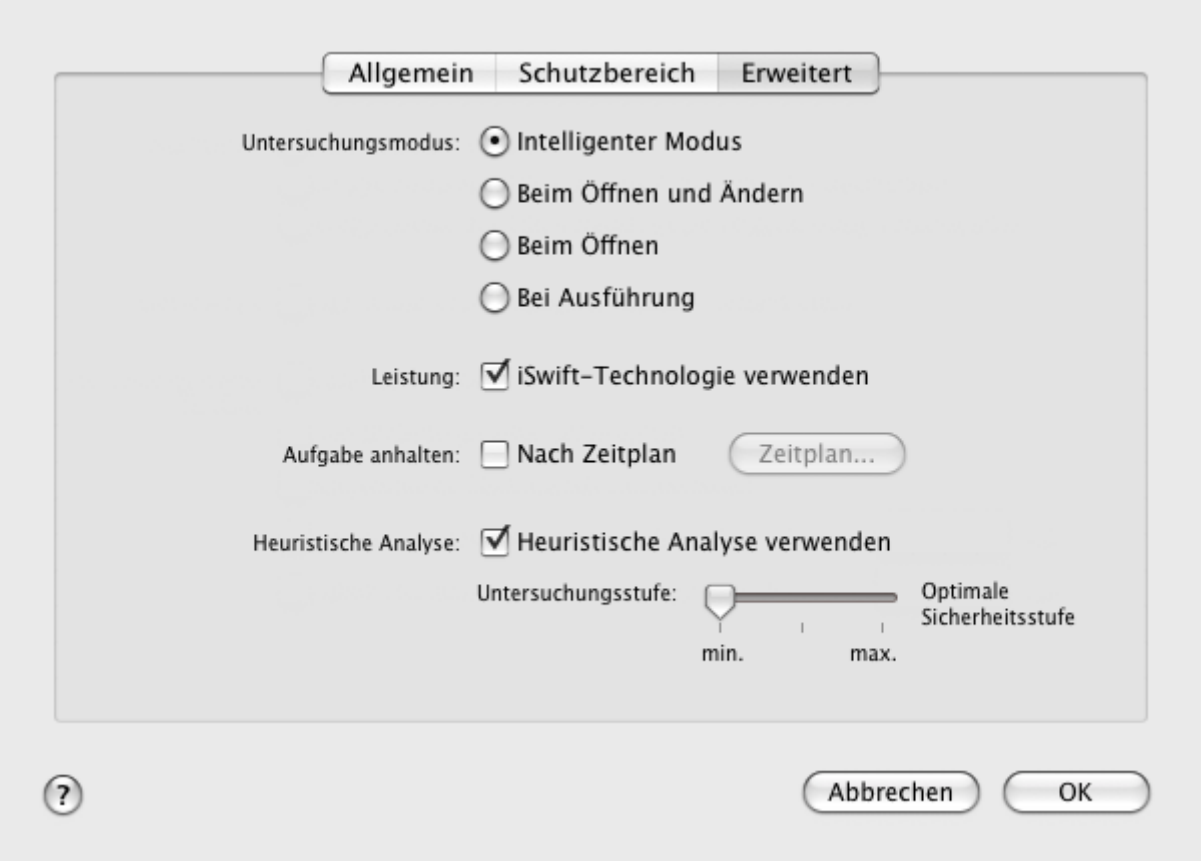

Abbildung 26. Datei-Anti-Virus: Zusätzliche Parameter anpassen

AKTION FÜR OBJEKTE AUSWÄHLEN

Wenn sich durch die Virenuntersuchung einer Datei herausstellt, dass sie infiziert oder verdächtig ist, hängt das weitere Vorgehen von Datei-Anti-Virus vom Status des Objekts und von der ausgewählten Aktion ab.

Ein Objekt kann aufgrund der Untersuchung einen der folgenden Status erhalten:

- Schädlich, Beispiele hierfür lauten *Virus* oder *trojanisches Programm*;
- *möglicherweise infiziert*, wenn sich aufgrund der Untersuchung nicht eindeutig feststellen lässt, ob das Objekt infiziert ist oder nicht. Das bedeutet, dass in der Datei die Codefolge eines unbekannten Virus oder der modifizierte Code eines bekannten Virus gefunden wurde.

Standardmäßig werden alle schädlichen Objekte der Desinfektion unterzogen und alle möglicherweise infizierten Objekte in die Quarantäne (siehe Abschnitt "Quarantäne" auf Seite 93) verschoben.

Um auszuwählen, welche Aktion Datei-Anti-Virus beim Fund eines infizierten oder möglicherweise infizierten Objekts ausführen soll, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Programmkonfigurationsfenster (siehe Seite 35), und wählen Sie die Registerkarte **Schutz** (siehe Abbildung unten) aus.
2. Wählen Sie im Block **Aktion** die erforderliche Aktion für Datei-Anti-Virus aus.

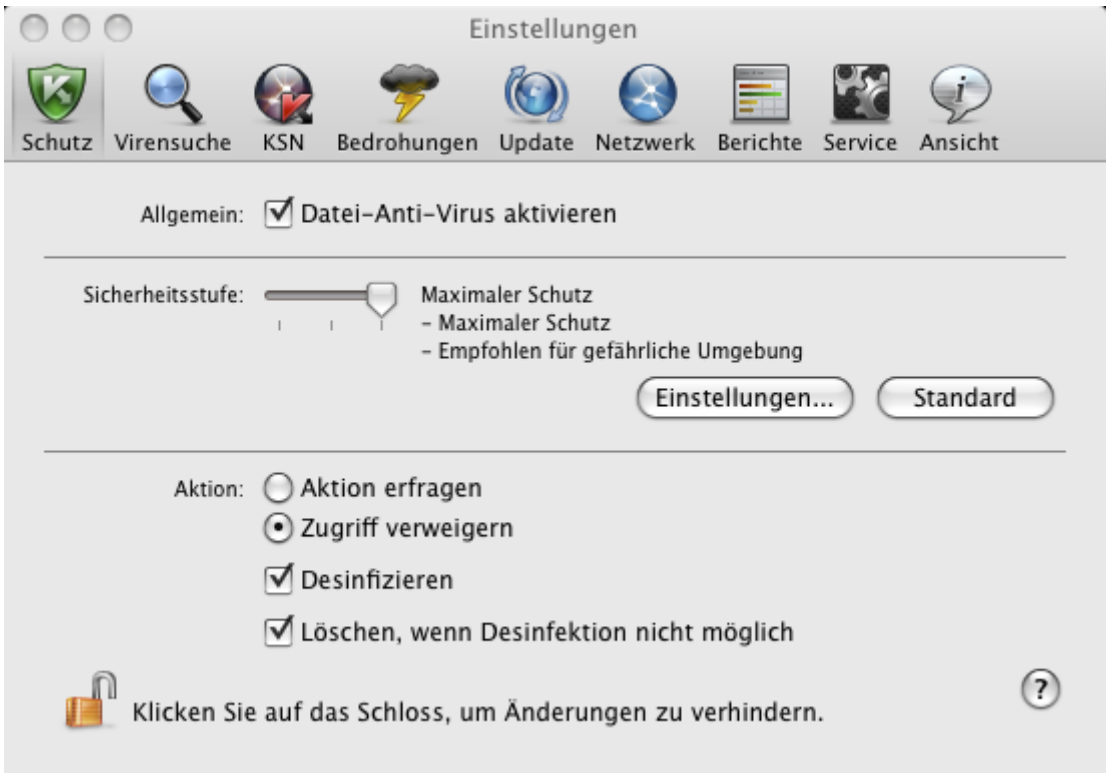

Abbildung 27. Programmkonfigurationsfenster. Schutz

Bevor ein Desinfektionsversuch erfolgt oder ein Objekt gelöscht wird, legt Kaspersky Anti-Virus eine Sicherungskopie des Objekts an und speichert diese im Backup (auf Seite 96). Dadurch kann das Objekt bei Bedarf wiederhergestellt oder später desinfiziert werden.

STANDARDPARAMETER FÜR DEN DATEISCHUTZ WIEDERHERSTELLEN

Sie können jederzeit zu den Standardeinstellungen von Datei-Anti-Virus zurückkehren. Diese gelten als optimal zum Schutz Ihres Computers vor schädlichen Programmen, werden von den Kaspersky-Lab-Spezialisten empfohlen und sind in der Sicherheitsstufe **Empfohlen** zusammengefasst.

Gehen Sie folgendermaßen vor, um die Standardeinstellungen für Datei-Anti-Virus wiederherzustellen:

1. Öffnen Sie das Programmkonfigurationsfenster (siehe Seite 35), und wählen Sie die Registerkarte **Schutz** (siehe Abbildung unten) aus.

2. Klicken Sie im Block **Sicherheitsstufe** auf die Schaltfläche **Standard**.

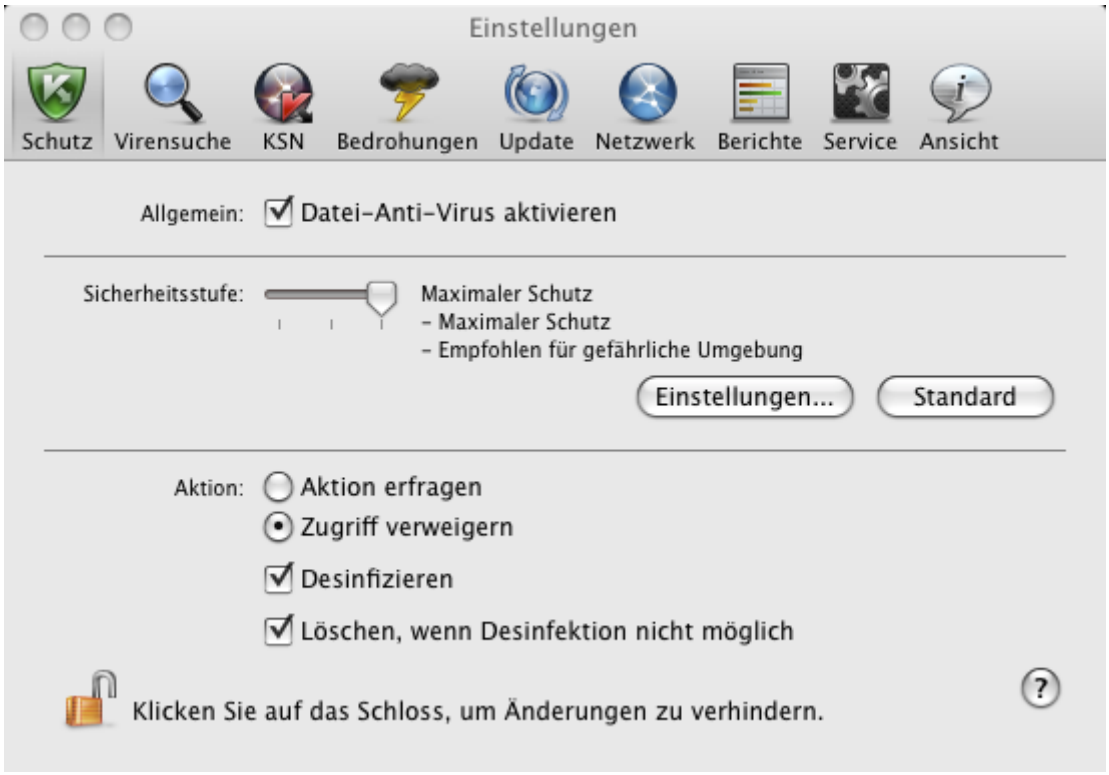

Abbildung 28. Programmkonfigurationsfenster. Schutz

STATISTIK ÜBER DEN DATEISCHUTZ

Eine zusammenfassende Statistik über die laufende Arbeit von Datei-Anti-Virus (Anzahl der Objekte, die seit dem letzten Start der Komponente untersucht wurden, Anzahl der gefundenen und desinfizierten gefährlichen Objekte, Name der letzten untersuchten Datei) wird im unteren Bereich des Programmhauptfensters (siehe Abschnitt "Programmhauptfenster" auf Seite 34) angezeigt.

Außerdem stellt Kaspersky Anti-Virus einen ausführlichen Bericht über die Arbeit von Datei-Anti-Virus bereit.

Gehen Sie folgendermaßen vor, um einen Bericht anzuzeigen:

1. Öffnen Sie das Programmhauptfenster (siehe Seite 34), und klicken Sie auf die Schaltfläche .

2. Wählen Sie im Abschnitt **Auszuführende Aufgaben** des folgenden Berichtfensters **Datei-Anti-Virus** aus.

Wenn Datei-Anti-Virus momentan deaktiviert ist, können Sie den Detailbericht über die Ergebnisse des letzten Starts der Komponente im Abschnitt **Abgeschlossene Aufgaben** anzeigen.

Wenn Datei-Anti-Virus fehlerhaft gearbeitet hat, lesen Sie den Bericht und versuchen, die Komponente noch einmal aufzurufen. Wenn es Ihnen nicht gelingt, das Problem selbst zu lösen, wenden Sie sich an den technischen Support von Kaspersky Lab (siehe Abschnitt "Kontaktaufnahme mit dem technischen Support" auf Seite 113).

Ausführliche Informationen über die Arbeit von Datei-Anti-Virus werden im rechten Teil des Berichtsfensters auf den folgenden Registerkarten angezeigt:

- Auf der Registerkarte **Gefunden** werden alle gefährlichen Objekte aufgeführt, die beim Schutz des Dateisystems gefunden wurden. Für jedes Objekt sind der Name, der Pfad zu dem Ordner, in dem das Objekt gespeichert wird, sowie der Status angegeben, der ihm von Datei-Anti-Virus zugewiesen wurde. Wenn genau festgestellt werden konnte, von welcher Malware das Objekt befallen ist, wird der entsprechende Status vergeben (z.B. *Virus*, *Trojanisches Programm* usw). Wenn der Malware-Typ nicht genau festgestellt werden konnte, erhält das Objekt den Status "*möglicherweise infiziert*". Neben dem Status wird außerdem die Aktion genannt, die mit dem Objekt ausgeführt wurde (*gefunden*, *nicht gefunden*, desinfiziert).

- Auf der Registerkarte **Ereignisse** ist eine vollständige Liste der von Datei-Anti-Virus registrierten Ereignisse aufgeführt. Die Liste enthält auch die folgenden Angaben zu den Ereignissen: Eintrittszeitpunkt, Namen, Status und Gründe für das Eintreten der Ereignisse. Die Ereignisse können folgende Status aufweisen:

  - Informatives Ereignis (z.B. *Objekt wurde nicht verarbeitet: nach Typ übersprungen*)

  - Warnung (z.B. *Virus gefunden*)

  - Hinweis (z.B. *Archiv ist kennwortgeschützt*).

- Auf der Registerkarte **Statistik** wird die Gesamtzahl der untersuchten Objekte angezeigt. Einzelne Spalten enthalten Informationen darüber, wie viele Archive und gefährliche Objekte sich unter den untersuchten Objekten befinden, wie viele Objekte desinfiziert oder in die Quarantäne verschoben sind usw.

- Auf der Registerkarte **Einstellungen** werden die wichtigsten Einstellungen angezeigt, mit denen Datei-Anti-Virus funktioniert. Um schnell zur Komponentenkonfiguration zu wechseln, klicken Sie auf die Schaltfläche **Einstellungen ändern**.

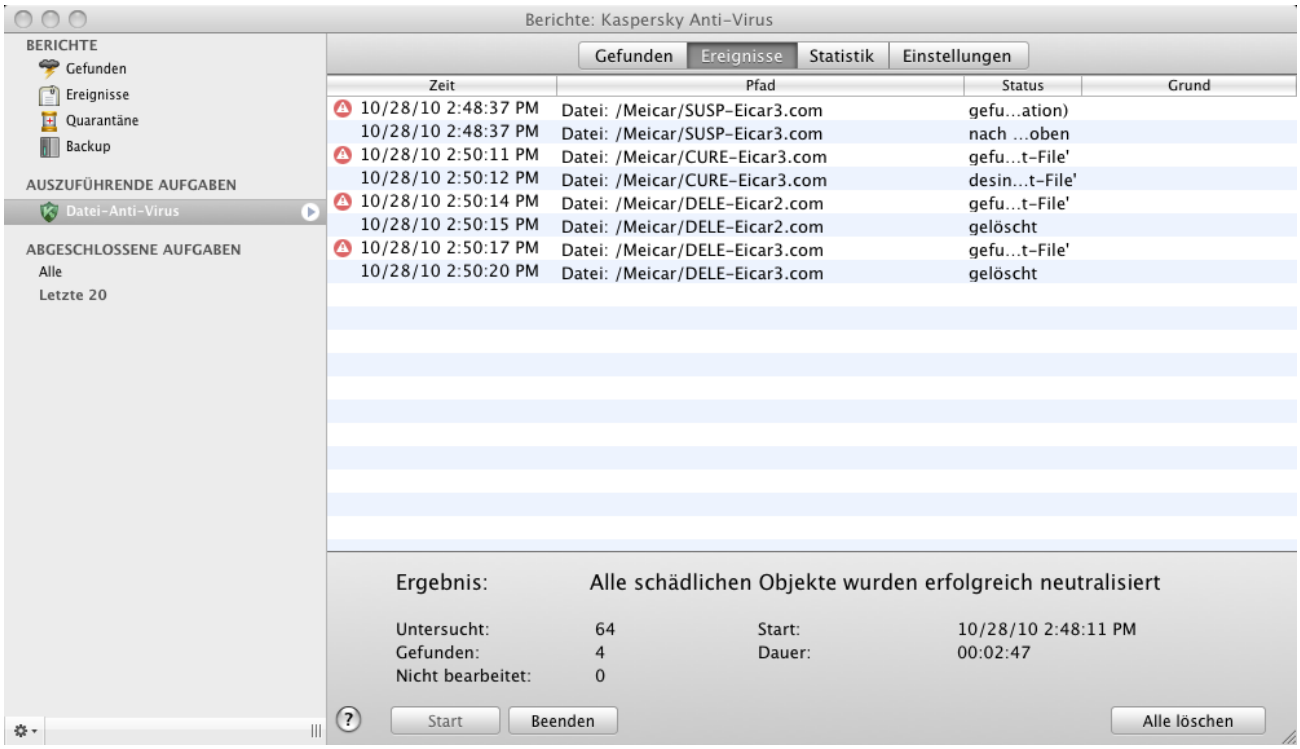

Abbildung 29. Berichtsfenster. Datei-Anti-Virus

VIRENSUCHE

Neben dem Echtzeitschutz des Computers durch die Komponente Datei-Anti-Virus (siehe Abschnitt "Datei-Anti-Virus" auf Seite 56) ist es sehr wichtig, Ihren Computer regelmäßig auf Viren zu untersuchen. Das ist erforderlich, um die Ausbreitung schädlicher Programme auszuschließen, die nicht von Datei-Anti-Virus erkannt wurden, weil beispielsweise eine zu geringe Sicherheitsstufe eingestellt war.

Kaspersky Anti-Virus bietet folgende Aufgaben zur Virensuche:

- **Virensuche**

  Virenuntersuchung eines einzelnen Objektes (Datei, Ordner, Datenträger, Wechselmedium).

- **Vollständige Suche**

  Virensuche auf Ihrem Computer mit ausführlicher Untersuchung aller Festplatten.

- **Schnelle Suche**

  Virenuntersuchung von kritischen Computerbereichen: Ordner, die Dateien des Betriebssystems und Systembibliotheken enthalten.

Diese Aufgaben werden standardmäßig mit den empfohlenen Einstellungen ausgeführt. Sie können diese Einstellungen ändern (siehe Abschnitt "Untersuchungsaufgaben anpassen" auf Seite 74) sowie einen Zeitplan für den Start der Untersuchungsaufgaben einrichten (siehe Abschnitt "Zeitplan für den Start der Untersuchungsaufgaben anpassen" auf Seite 78).

IN DIESEM ABSCHNITT

Aufgabenverwaltung Virensuche 68

Liste der Untersuchungsobjekte erstellen 72

Untersuchungsaufgaben anpassen 74

Standardmäßige Untersuchungseinstellungen wiederherstellen 80

Statistik über die Virensuche 81

AUFGABENVERWALTUNG VIRENSUCHE

Untersuchungsaufgaben können manuell (siehe Abschnitt "Untersuchungsaufgaben starten / beenden" auf Seite 69) oder automatisch nach Zeitplan gestartet werden (siehe Abschnitt "Zeitplan für den Start der Untersuchungsaufgaben anpassen" auf Seite 78). Außerdem besteht in Kaspersky Anti-Virus die Möglichkeit, benutzerdefinierte Aufgaben zu erstellen (siehe Abschnitt "Untersuchungsaufgaben erstellen" auf Seite 70).

UNTERSUCHUNGSAUFGABEN STARTEN / BEENDEN

Um eine Untersuchungsaufgabe manuell zu starten, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Programmhauptfenster (siehe Seite 34), und klicken Sie auf die Schaltfläche .

2. Wählen Sie im folgenden Fenster (siehe Abbildung unten) die gewünschte Aufgabe aus: **Vollständige Suche**, **Schnelle Suche** oder **Virensuche**. Wenn Sie die Aufgabe **Virensuche** ausgewählt haben, werden Sie aufgefordert, einen Untersuchungsbereich festzulegen. Neben den genannten Aufgaben, die zum Lieferumfang des Programms gehören, werden benutzerdefinierte Aufgaben zur Virensuche im Menü angezeigt (siehe Abschnitt "Untersuchungsaufgaben erstellen" auf Seite 70), wenn diese erstellt worden sind.

Abbildung 30. Aufgaben zur Virensuche

Informationen über momentan laufende Aufgaben werden auf der linken Seite des Hauptfensters sowie im Abschnitt **Auszuführende Aufgaben** des Berichtsfensters angezeigt (siehe Abschnitt Berichte auf Seite 98). Die Informationen über die ausgeführten Aufgaben werden im Berichtsfenster im Abschnitt **Abgeschlossene Aufgaben** angezeigt (siehe Abbildung unten).

Um eine Untersuchungsaufgabe zu beenden, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Programmhauptfenster (siehe Seite 34), und klicken Sie auf die Schaltfläche . Daraufhin wird das Berichtsfenster von Kaspersky Anti-Virus geöffnet.

2. Wählen Sie im Abschnitt **Auszuführende Aufgaben** den Namen der gewünschten Aufgabe zur Virensuche aus (siehe Abbildung unten), und klicken Sie auf die Schaltfläche **Anhalten**. Die Untersuchung wird angehalten, bis die Aufgabe erneut manuell oder nach Zeitplan gestartet wird. Um eine neue Untersuchung zu starten, klicken Sie auf die Schaltfläche **Start**. Daraufhin wird das Fenster geöffnet, in dem Sie aufgefordert werden, die abgebrochene Untersuchung fortzusetzen oder eine neue Untersuchung zu starten.

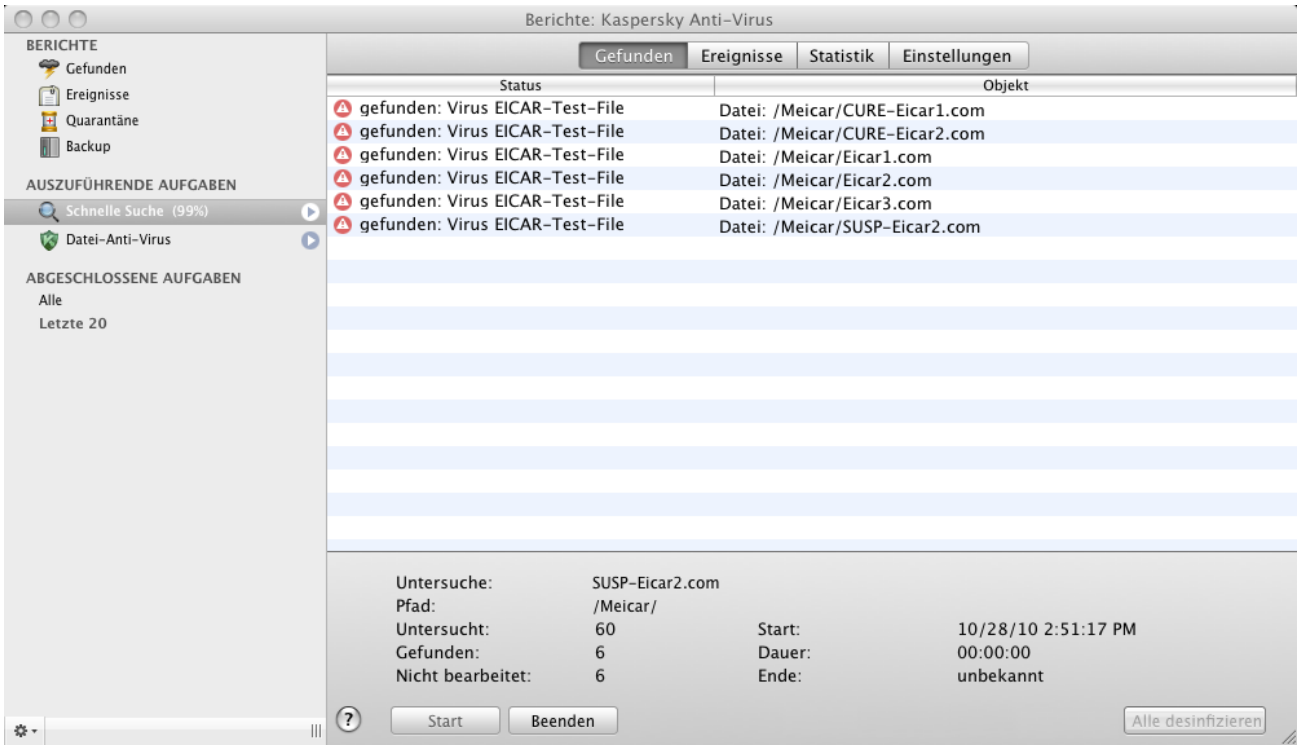

Abbildung 31. Berichtsfenster. Virensuche

UNTERSUCHUNGSAUFGABEN ERSTELLEN

Für eine Virenprüfung der Objekte auf dem Computer können Sie nicht nur die in Kaspersky Anti-Virus vorhandenen Aufgaben zur Virensuche verwenden, sondern auch eigene Aufgaben erstellen. Eine neue Aufgabe wird auf Grundlage einer vorhandenen Untersuchungsaufgabe erstellt.

Um eine neue Untersuchungsaufgabe zu erstellen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Programmkonfigurationsfenster (auf Seite 35).

2. Wählen Sie die Registerkarte **Virensuche** und dann in der linken Liste (siehe Abbildung unten) die Aufgabe **Schnelle Suche** oder **Vollständige Suche** aus, deren Einstellungen Ihren Anforderungen am nächsten kommen.

Abbildung 32. Programmkonfigurationsfenster. Aufgabe Vollständige Suche

3. Klicken Sie auf die Schaltfläche , die sich unter der Liste mit Aufgaben zur Virensuche befindet, und wählen Sie im folgenden Menü den Befehl **Kopieren** aus.

4. Geben Sie im folgenden Fenster einen Namen für die neue Aufgabe ein, und klicken Sie auf **OK**. Die Aufgabe erscheint in der Aufgabenliste unter dem angegebenen Namen.

Die neue Aufgabe übernimmt alle Einstellungen der Aufgabe, auf deren Grundlage sie erstellt wurde. Deshalb können erweiterte Einstellungen erforderlich sein:

- Liste der Untersuchungsobjekte ändern (siehe Abschnitt "Liste der Untersuchungsobjekte erstellen" auf Seite 72)
- Einstellungen festlegen (siehe Abschnitt "Untersuchungsaufgaben anpassen" auf Seite 74), mit denen die Aufgabe ausgeführt werden soll
- Zeitplan für den automatischen Aufgabenstart anpassen (siehe Abschnitt "Startmodus für die Aufgaben zur Virensuche anpassen" auf Seite 78).

Außerdem ermöglicht Kaspersky Anti-Viruszusätzlich zu den vorhandenen Aufgaben zur Virensuche das Erstellen von maximal sechs benutzerdefinierten Aufgaben zur Virensuche.

Sie können die Suchaufgaben umbenennen oder löschen.

Es lassen sich nur die Aufgaben umbenennen und löschen, die vom Benutzer erstellt wurden.

Um eine Untersuchungsaufgabe umzubenennen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Programmkonfigurationsfenster (auf Seite 35).
2. Wählen Sie in der linken Liste eine Aufgabe aus (siehe Abbildung oben).
3. Klicken Sie auf die Schaltfläche , die sich unter der Liste mit Untersuchungsaufgaben befindet, und wählen Sie im folgenden Menü den Befehl **Umbenennen** aus.
4. Ändern Sie im folgenden Fenster den Namen der Aufgabe, und klicken Sie auf **OK**. Die Aufgabe wird umbenannt.

Um eine Untersuchungsaufgabe zu löschen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Programmkonfigurationsfenster (auf Seite 35).
2. Wählen Sie in der linken Liste eine Aufgabe aus (siehe Abbildung oben).
3. Klicken Sie auf die Schaltfläche , die sich unter der Liste mit Untersuchungsaufgaben befindet, und wählen Sie im folgenden Menü den Befehl **Löschen** aus. Bestätigen Sie die Aktion im folgenden Fenster. Die Aufgabe wird aus der Aufgabenliste gelöscht.

LISTE DER UNTERSUCHUNGSOBJEKTE ERSTELLEN

Für die Aufgaben **Vollständige Suche** und **Schnelle Suche** gibt es in Kaspersky Anti-Virus bereits erstellte Listen der Untersuchungsobjekte. Die Aufgabe **Vollständige Suche** ermöglicht die Untersuchung aller Dateien auf allen Festplatten des Computers. Wenn Kaspersky Anti-Virus die Aufgabe**Schnelle Suche** durchführt, werden nur die aus Sicht der Sicherheit anfälligen Objekte untersucht: Ordner, die Dateien des Betriebssystems enthalten und Systembibliotheken.

Für die Ausführung der Aufgabe **Virensuche** ist es erforderlich, eine Liste der Untersuchungsobjekte zu erstellen (zur Auswahl einer Datei, eines Ordners, Laufwerks oder eines Wechseldatenträgers).

*Um die Liste der Untersuchungsobjekte bei der Ausführung der Aufgaben **Vollständige Suche** und **Schnelle Suche** anzuzeigen oder zu ändern, gehen Sie folgendermaßen vor:*

1. Öffnen Sie das Programmkonfigurationsfenster (siehe Seite 35), und wählen Sie die Registerkarte **Virensuche** aus.
2. Wählen Sie in der linken Liste die gewünschte Aufgabe aus: **Vollständige Suche** oder **Schnelle Suche**.
3. Klicken Sie im Block rechts **Zu untersuchende Objekte** auf die Schaltfläche **Ändern**. Daraufhin wird ein Fenster mit der Liste der Objekte geöffnet (siehe Abbildung unten). Ändern Sie die Liste bei Bedarf.

   Sie können folgende Aktionen ausführen:

   - Objekte der Liste hinzufügen.

     Verschieben Sie ein Objekt in das Fenster, oder klicken Sie auf die Schaltfläche , und wählen Sie aus der Dropdown-Liste die passende Variante aus (**Datei oder Ordner**, **Alle Laufwerke**, **Quarantäne** usw.). Wenn ein hinzuzufügendes Objekt untergeordnete Ordner enthält, die auch untersucht werden sollen, aktivieren Sie im geöffneten Fenster zur Dateiauswahl das Kontrollkästchen **Unterordner einschließen**. Wenn das hinzuzufügende Objekt symbolische Links auf andere Objekte enthält, die untersucht werden sollen, aktivieren Sie im folgenden Fenster zur Dateiauswahl das Kontrollkästchen **Zwischen symbolischen Links wechseln**.

- Objekte in der Liste ändern (Dies ist nur für die Objekte verfügbar, die der Benutzer hinzugefügt hat).

  Wählen Sie ein Objekt aus, und klicken Sie auf die Schaltfläche **Ändern**. Nehmen Sie im folgenden Fenster die erforderlichen Änderungen vor.

- Bestimmte Objekte der Liste vorübergehend von der Untersuchung ausschließen.

  Wählen Sie ein Objekt aus, und deaktivieren Sie das entsprechende Kontrollkästchen. Die Aufgabe zur Virensuche wird für dieses Objekt solange nicht ausgeführt, bis das Kontrollkästchen wieder aktiviert ist.

- Objekte löschen (Dies ist nur für die Objekte verfügbar, die der Benutzer hinzugefügt hat).

  Wählen Sie ein Objekt aus, und klicken Sie auf die Schaltfläche .

Beim Erstellen benutzerdefinierter Aufgaben (siehe Abschnitt "Untersuchungsaufgaben erstellen" auf Seite 70) wird die Liste der Untersuchungsobjekte auf ähnliche Weise erstellt oder geändert.

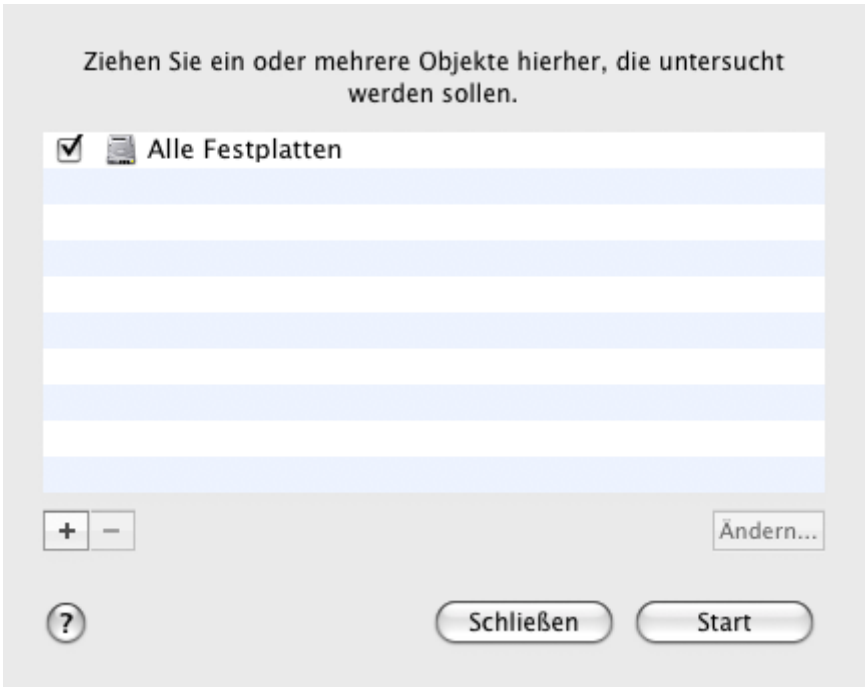

Abbildung 33. Liste der Untersuchungsobjekte erstellen

*Um ein oder mehrere Untersuchungsobjekte bei der Ausführung der Aufgabe zur **Virensuche**, gehen Sie wie folgt vor:*

1. Öffnen Sie das Programmhauptfenster (siehe Seite 34), und klicken Sie auf die Schaltfläche .

2. Wählen Sie im folgenden Menü die Aufgabe **Virensuche** aus. Daraufhin wird das Fenster für die Erstellung einer Liste der Objekte geöffnet (siehe Abbildung oben). Bearbeiten Sie die Liste mit der oben beschriebenen Methode.

UNTERSUCHUNGSAUFGABEN ANPASSEN

Die Ausführung der Aufgaben zur Virensuche auf Ihrem Computer wird durch die folgenden Einstellungen definiert:

- **Sicherheitsstufe**

  Die Sicherheitsstufe entspricht einer Auswahl von Parametern, die das Verhältnis zwischen der Genauigkeit und der Geschwindigkeit der Objektuntersuchung bestimmen. Drei vordefinierte Sicherheitsstufen (siehe Abschnitt "Sicherheitsstufe auswählen" auf Seite 74) sind verfügbar, deren Einstellungen die Spezialisten von Kaspersky Lab erarbeitet haben.

- **Aktion für ein gefundenes Objekt**

  Die Aktion (siehe Abschnitt "Aktion für Objekte auswählen" auf Seite 77) bestimmt, wie Kaspersky Anti-Virus beim Fund eines infizierten oder möglicherweise infizierten Objekts reagiert.

- **Startmodus**

  Der automatische Start der Aufgaben zur Virensuche nach einem festgelegten Zeitplan (siehe Abschnitt "Startmodus für die Untersuchungsaufgaben nach Zeitplan anpassen" auf Seite 78) ermöglicht es Ihnen, Ihren Computer rechtzeitig auf Viren zu untersuchen. Dies ist nur für die Aufgaben **Schnelle Suche**, **Vollständige Suche** und für die benutzerdefinierten Aufgaben verfügbar.

- **Aufgabenstart unter Benutzernamen**

  Der Start einer Aufgabe unter dem Root-Benutzer (siehe Abschnitt "Untersuchungsaufgaben unter Benutzernamen starten" auf Seite 78) ermöglicht eine rechtzeitige Untersuchung unabhängig davon, über welche Rechte der Benutzer verfügt, der momentan am Computer arbeitet. Dies ist nur für die Aufgaben **Schnelle Suche**, **Vollständige Suche** und für die benutzerdefinierten Aufgaben verfügbar.

Außerdem können Sie einheitliche Werte für die Parameter **Sicherheitsstufe** und **Aktion** für alle Aufgaben zur Virensuche festlegen (siehe Abschnitt "Einheitliche Untersuchungsparameter für alle Aufgaben zur Virensuche festlegen" auf Seite 79).

SICHERHEITSSTUFE AUSWÄHLEN

Für eine Aufgabe zur Virensuche stehen folgende Stufen zur Auswahl:

- **Maximaler Schutz**: Auf dieser Stufe erfolgt die Untersuchung des gesamten Computers oder eines Laufwerks, Ordners oder einer Datei des Computers mit maximaler Ausführlichkeit. Es wird empfohlen, diese Stufe zu verwenden, wenn Sie vermuten, dass Ihr Computer mit einem Virus infiziert ist.

- **Empfohlen**: Die Einstellungen dieser Stufe werden von den Kaspersky-Lab-Spezialisten empfohlen.

- **Maximales Tempo**: Diese Stufe erlaubt Ihnen, komfortabel mit Anwendungen zu arbeiten, die den Arbeitsspeicher stark beanspruchen, weil die Auswahl der zu untersuchenden Dateien auf dieser Stufe eingeschränkt wird.

Standardmäßig werden die Aufgaben zur Virensuche auf der Sicherheitsstufe **Empfohlen** ausgeführt. Sie können die Genauigkeit der Untersuchung der Objekte erhöhen oder senken, indem Sie die Stufe **Maximaler Schutz** bzw. **Maximales Tempo** auswählen oder Einstellungen der aktuellen Stufe anpassen.

Um die aktuelle Sicherheitsstufe für eine Aufgabe zur Virensuche zu ändern, gehen Sie folgendermaßen vor:

1. Öffnen Sie Öffnen Sie das Programmkonfigurationsfenster (siehe Seite 35), und wählen Sie die Registerkarte **Virensuche** aus (siehe Abbildung oben).
2. Wählen Sie in der linken Liste die Aufgabe aus.
3. Verschieben Sie den Schieberegler auf der Skala im Block **Sicherheitsstufe**. Durch das Anpassen der Sicherheitsstufe wird das Verhältnis zwischen der Ausführungsgeschwindigkeit der Untersuchung und der Anzahl der zu untersuchenden Dateien bestimmt: Je weniger Dateien der Virenanalyse unterzogen werden, desto höher ist die Untersuchungsgeschwindigkeit.

Wenn keine der vordefinierten Sicherheitsstufen Ihren Anforderungen entspricht, können Sie die Schutzparameter zusätzlich anpassen. Wählen Sie dazu die Sicherheitsstufe aus, die Ihren Anforderungen am nächsten kommt, und passen Sie ihre Einstellungen entsprechend an. In diesem Fall ändert sich der Name der Sicherheitsstufe in **Benutzerdefiniert**.

Um die Einstellungen der aktuellen Sicherheitsstufe anzupassen, gehen Sie folgendermaßen vor:

1. Öffnen Sie Öffnen Sie das Programmkonfigurationsfenster (siehe Seite 35), und wählen Sie die Registerkarte **Virensuche** aus (siehe Abbildung oben).
2. Wählen Sie in der linken Liste die Aufgabe aus.
3. Klicken Sie im Block **Sicherheitsstufe** auf die Schaltfläche **Einstellungen**.
4. Passen Sie im folgenden Fenster die Parameter (siehe Abschnitt "Typen der zu untersuchenden Objekte festlegen" auf Seite 76) für die Sicherheitsstufe an, und klicken Sie auf die Schaltfläche **OK**, um die Änderungen zu sichern.

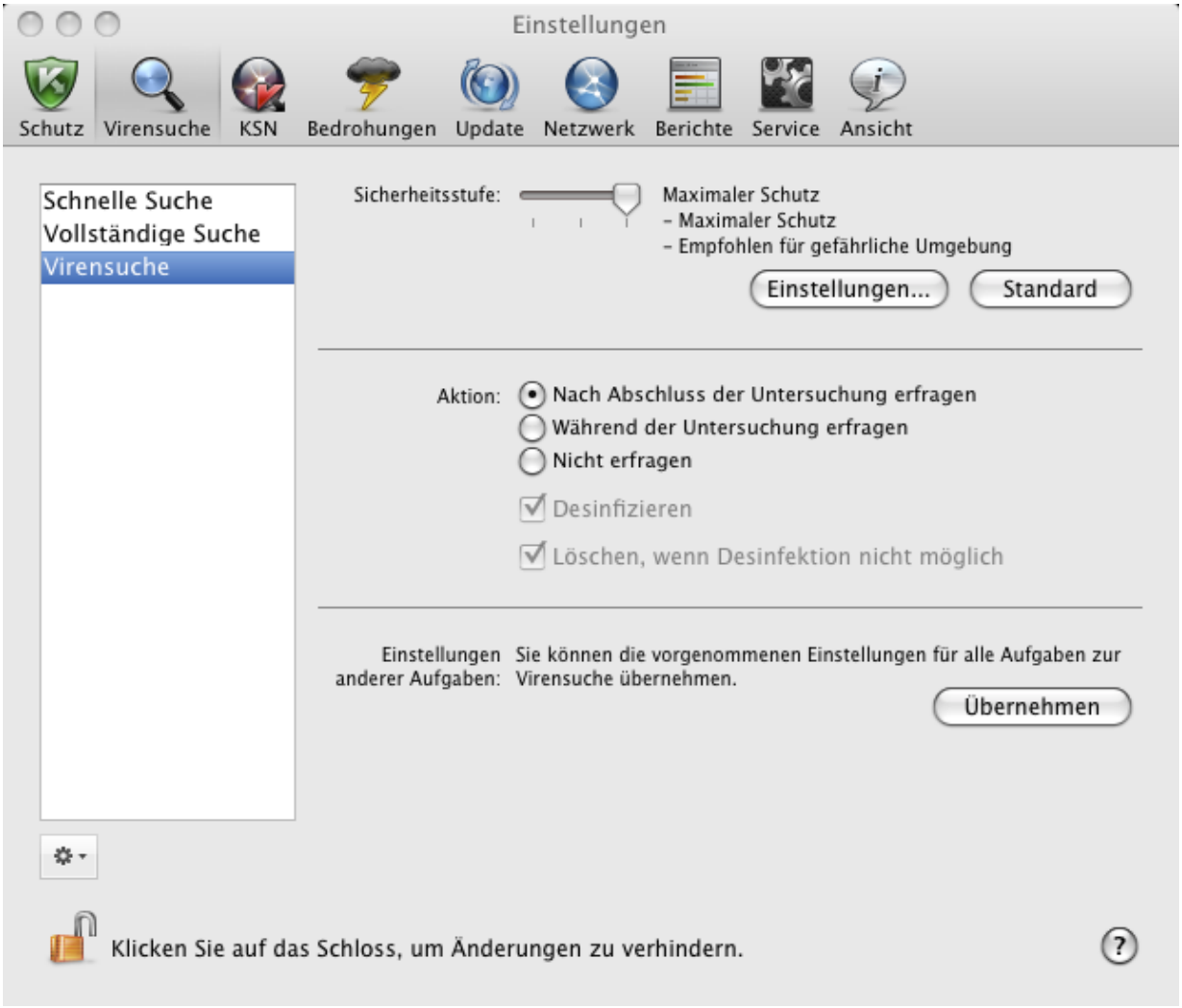

Abbildung 34. Programmkonfigurationsfenster. Aufgabe Virensuche

TYPEN DER ZU UNTERSUCHENDEN OBJEKTE FESTLEGEN

Durch die Angabe des Typs der zu untersuchenden Objekte bestimmen Sie das Format und die Größe der Dateien, die von Kaspersky Anti-Virus bei der Ausführung dieser Aufgabe untersucht werden sollen.

Um den Typ der Objekte festzulegen, die bei der Ausführung der Aufgabe zur Virensuche untersucht werden sollen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Programmkonfigurationsfenster (siehe Seite 35), und wählen Sie die Registerkarte **Virensuche** aus.
2. Wählen Sie in der linken Liste die Aufgabe aus.
3. Klicken Sie im Block **Sicherheitsstufe** auf die Schaltfläche **Einstellungen**. Passen Sie im folgenden Fenster (siehe Abbildung unten) die folgenden Parameter an:
   - Geben Sie im Block **Dateitypen** den Format der Dateien an, die von Kaspersky Anti-Virus bei der Ausführung der Untersuchungsaufgaben untersucht werden.
   - Passen Sie im Block **Optimierung** die Leistungsfähigkeit der Suche und die Verwendung der Suchtechnologie an.
   - Wählen Sie im Block **Zusammengesetzte Dateien** die zusammengesetzten Dateien aus, die auf Viren untersucht werden sollen.
   - Passen Sie im Block **Heuristische Analyse** die Verwendung der heuristischen Analyse in Untersuchungsaufgaben an.

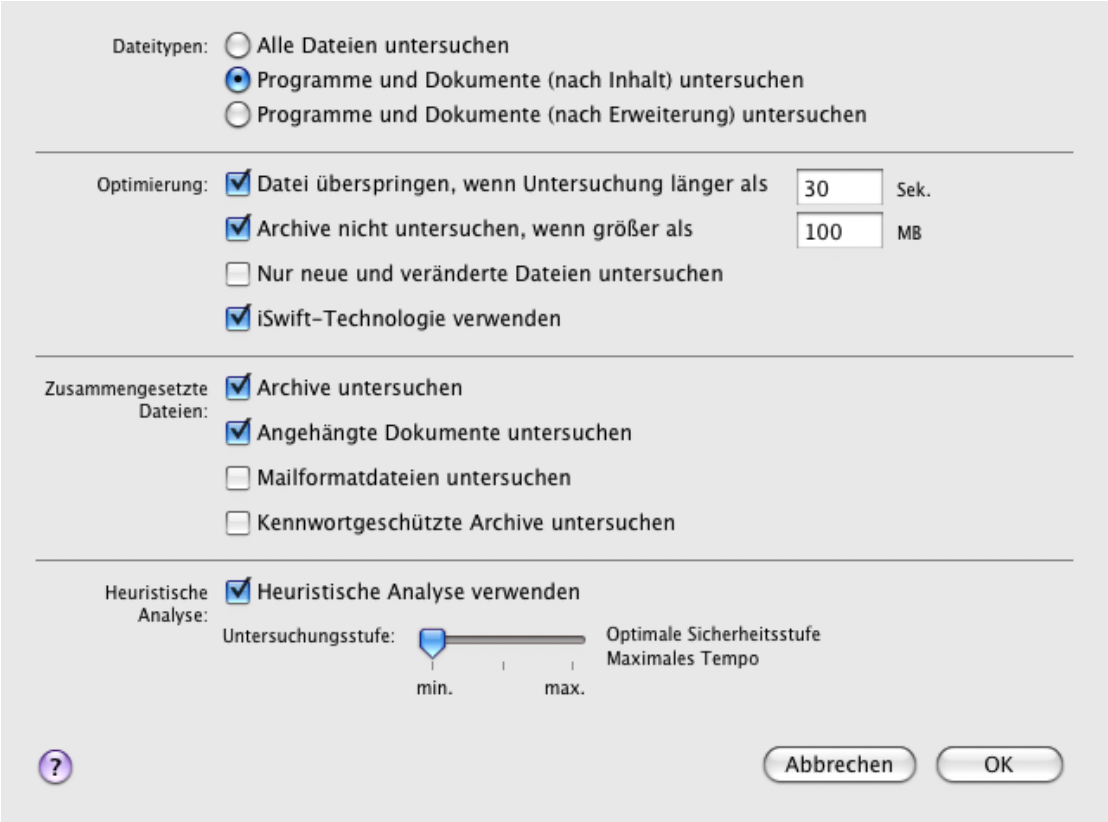

Abbildung 35. Virensuche: Untersuchungsparameter anpassen

AKTION FÜR OBJEKTE AUSWÄHLEN

Wenn es sich aufgrund der Ausführung einer Aufgabe zur Virensuche herausstellt, dass ein Objekt infiziert oder möglicherweise infiziert ist, hängt das weitere Vorgehen von Kaspersky Anti-Virus von dem Status des Objekts und der ausgewählten Aktion ab.

Ein Objekt kann aufgrund der Untersuchung einen der folgenden Status erhalten:

- Schädlich, Beispiele hierfür lauten *Virus* oder *trojanisches Programm*;
- *möglicherweise infiziert*, wenn sich aufgrund der Untersuchung nicht eindeutig feststellen lässt, ob das Objekt infiziert ist oder nicht. Das bedeutet, dass in der Datei die Codefolge eines unbekannten Virus oder der modifizierte Code eines bekannten Virus gefunden wurde.

Standardmäßig werden alle schädlichen Objekte der Desinfektion unterzogen und alle möglicherweise infizierten Objekte in die Quarantäne (siehe Abschnitt "Quarantäne" auf Seite 93) verschoben.

Um auszuwählen, welche Aktion Kaspersky Anti-Virus beim Fund eines infizierten oder möglicherweise infizierten Objekts ausführen soll, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Programmkonfigurationsfenster (auf Seite 35), wählen Sie die Registerkarte **Virensuche** und in der linken Liste den Namen der gewünschten Aufgabe zur Virensuche aus (siehe Abbildung unten).
2. Wählen Sie im Block **Aktion** die erforderliche Aktion für Kaspersky Anti-Virus aus.

Abbildung 36. Programmkonfigurationsfenster. Aufgabe Vollständige Suche

Bevor ein Desinfektionsversuch erfolgt oder ein Objekt gelöscht wird, legt Kaspersky Anti-Virus eine Sicherungskopie des Objekts an und speichert diese im Backup (auf Seite 96). Dadurch kann das Objekt bei Bedarf wiederhergestellt oder später desinfiziert werden.

START DER AUFGABEN ZUR VIRENSUCHE NACH ZEITPLAN ANPASSEN

Sie können alle Aufgaben zur Virensuche auf Ihrem Computer manuell ausführen (siehe Abschnitt "Untersuchungsaufgaben starten / beenden" auf Seite 69). Außerdem können die Aufgaben **Schnelle Suche** und **Vollständige Suche** sowie die vom Benutzer erstellten Aufgaben nach einem im Voraus erstellten Zeitplan ausgeführt werden.

- *Um den Start für die Aufgaben **Schnelle Suche** und **Vollständige Suche** sowie für die benutzerdefinierten Aufgaben zur Virensuche nach Zeitplan anzupassen, gehen Sie folgendermaßen vor:*

1. Öffnen Sie das Programmkonfigurationsfenster (siehe Seite 35), und wählen Sie die Registerkarte **Virensuche** aus.

2. Wählen Sie in der linken Liste den Namen der gewünschten Untersuchungsaufgabe aus, und aktivieren Sie im Block **Startmodus** den Aufgabenstart nach Zeitplan. Klicken Sie auf die Schaltfläche **Ändern**, um die Parameter für den Aufgabenstart anzupassen.

3. Legen Sie im folgenden Fenster (siehe Abbildung unten) fest, mit welcher Frequenz die Aufgabe gestartet werden soll.

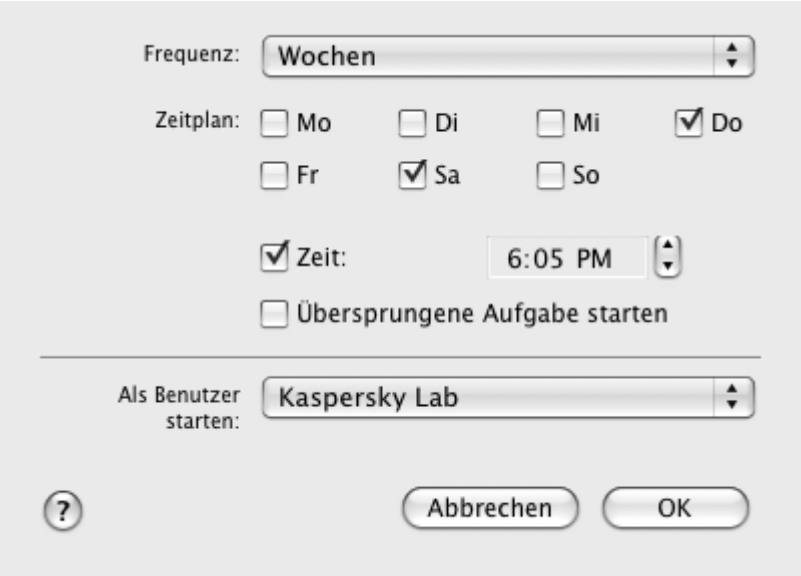

Abbildung 37. Startzeitplan einer Untersuchungsaufgabe anpassen

UNTERSUCHUNGSAUFGABEN UNTER BENUTZERNAMEN STARTEN

Das Programm verfügt über die Möglichkeit, die dem Benutzer erlaubt, die Aufgaben unter einem anderen Benutzerkonto zu starten. Dies ermöglicht eine rechtzeitige Untersuchung unabhängig davon, über welche Rechte der Benutzer verfügt, der momentan am Computer arbeitet. So können beispielsweise bei der Untersuchung Zugriffsrechte für ein zu untersuchendes Objekt erforderlich sein. Durch die Verwendung dieses Dienstes können Sie festlegen, dass die Aufgaben zur Virensuche unter dem Namen des Benutzers gestartet werden, der über solche Berechtigungen verfügt.

Standardmäßig ist dieser Dienst deaktiviert, und die Aufgaben werden unter dem aktuellen Benutzerkonto gestartet, unter dem Sie an dem System autorisiert sind.

Sie können den Start der Untersuchungsaufgaben unter dem Root-Benutzer nur für die Aufgaben **Schnelle Virensuche** und **Vollständige Virensuche** sowie für die anhand dieser Aufgaben erstellten benutzerdefinierten Aufgaben anpassen.

Um das Benutzerkonto festzulegen, unter dem die Aufgaben zur Virensuche ausgeführt werden sollen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Programmkonfigurationsfenster (siehe Seite 35), wählen Sie die Registerkarte **Virensuche** aus.

2. Wählen Sie in der linken Liste den Namen der gewünschten Untersuchungsaufgabe aus, und aktivieren Sie im Block **Startmodus** den Aufgabenstart nach Zeitplan. Klicken Sie auf die Schaltfläche **Ändern**, um den Aufgabenstart vom Benutzernamen aus anzupassen.

3. Wählen Sie im folgenden Fenster (siehe Abbildung unten) im Block **Als Benutzer starten** das Benutzerkonto aus, unter dessen Namen die Aufgabe gestartet werden soll.

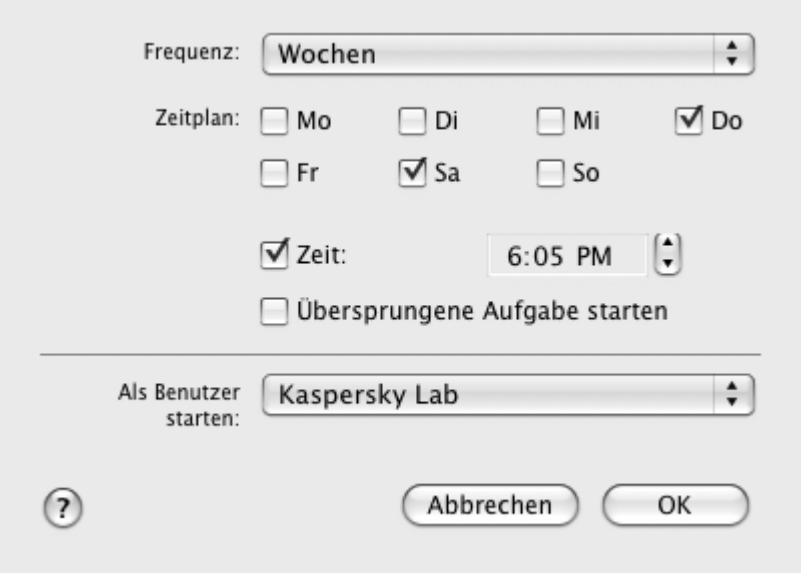

Abbildung 38. Startzeitplan einer Untersuchungsaufgabe anpassen

EINHEITLICHE UNTERSUCHUNGSPARAMETER FÜR ALLE AUFGABEN ZUR VIRENSUCHE FESTLEGEN

Standardmäßig werden die Untersuchungsaufgaben, die zum Lieferumfang von Kaspersky Anti-Virus gehören, entsprechend den von Kaspersky Lab empfohlenen Einstellungen ausgeführt. Die benutzerdefinierten Aufgaben zur Virensuche übernehmen dabei alle festgelegten Einstellungen. Sie können die Einstellungen (siehe Abschnitt "Untersuchungsaufgaben anpassen" auf Seite 74) für jede Untersuchungsaufgabe nicht nur einzeln anpassen, sondern auch einheitliche Einstellungen für alle Untersuchungsaufgaben festlegen. Als Grundlage dienen die Werte der Parameter **Sicherheitsstufe** und **Aktion** der Aufgabe **Virensuche**, die für die Untersuchung eines einzelnen Objekts vorgesehen ist.

Um einheitliche Untersuchungsparameter für alle Aufgaben festzulegen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Programmkonfigurationsfenster (siehe Seite 35), und wählen Sie die Registerkarte **Virensuche** aus.

2. Wählen Sie in der linken Liste die Aufgabe **Virensuche** aus (siehe Abbildung unten)**.**

3. Legen Sie die Sicherheitsstufe (siehe Abbildung "Sicherheitsstufe auswählen" auf Seite 74) fest, die Ihren Anforderungen am nächsten kommt, passen Sie ihre Parameter (siehe Abschnitt "Typen der zu untersuchenden Objekte festlegen" auf Seite 76) an, und wählen Sie die Aktion für infizierte bzw. möglicherweise infizierte Objekte (siehe Abschnitt "Aktion für Objekte auswählen" auf Seite 77) aus.

4. Klicken Sie im Block **Einstellungen anderer Aufgaben** auf die Schaltfläche **Übernehmen**. Kaspersky Anti-Virus wendet die Werte der Einstellungen **Schutzstufe** und **Aktion** auf andere, einschließlich benutzerdefinierte Aufgaben zur Virensuche an.

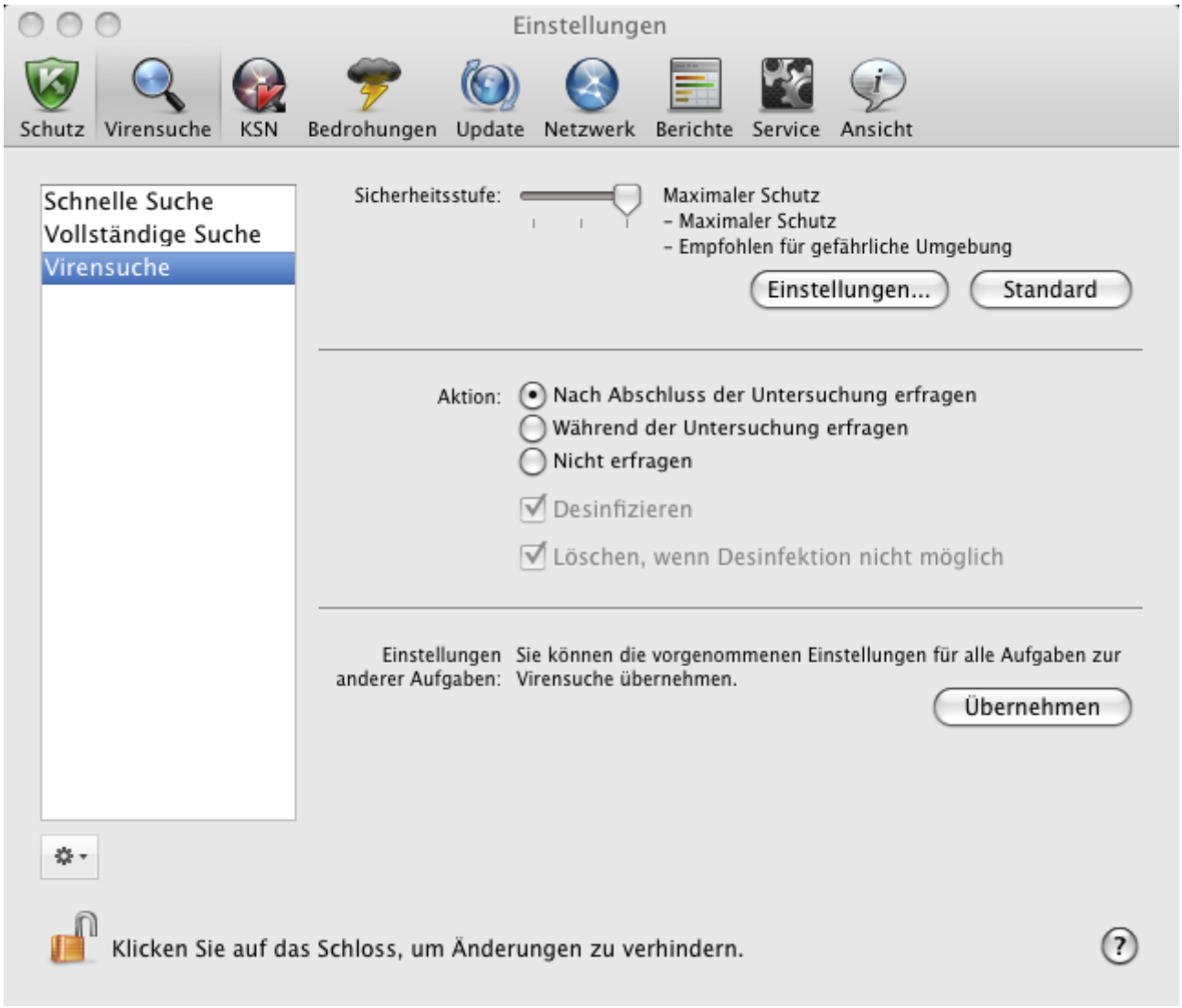

Abbildung 39. Programmkonfigurationsfenster. Aufgabe Virensuche

STANDARDMÄßIGE UNTERSUCHUNGSEINSTELLUNGEN WIEDERHERSTELLEN

Sie können jederzeit zu den Standardeinstellungen der Untersuchungsaufgaben zurückkehren. Diese gelten als optimal, werden von den Kaspersky-Lab-Spezialisten empfohlen und sind in der Sicherheitsstufe **Empfohlen** zusammengefasst.

Um die standardmäßigen Einstellungen für die Untersuchung von Objekten wiederherzustellen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Programmkonfigurationsfenster (auf Seite 35), wählen Sie die Registerkarte **Virensuche** und anschließend die entsprechende Aufgabe in der linken Liste aus.

2. Klicken Sie im Block **Sicherheitsstufe** (siehe Abbildung unten) auf die Schaltfläche **Standard**. Die empfohlenen Aufgabeneinstellungen werden wiederhergestellt.

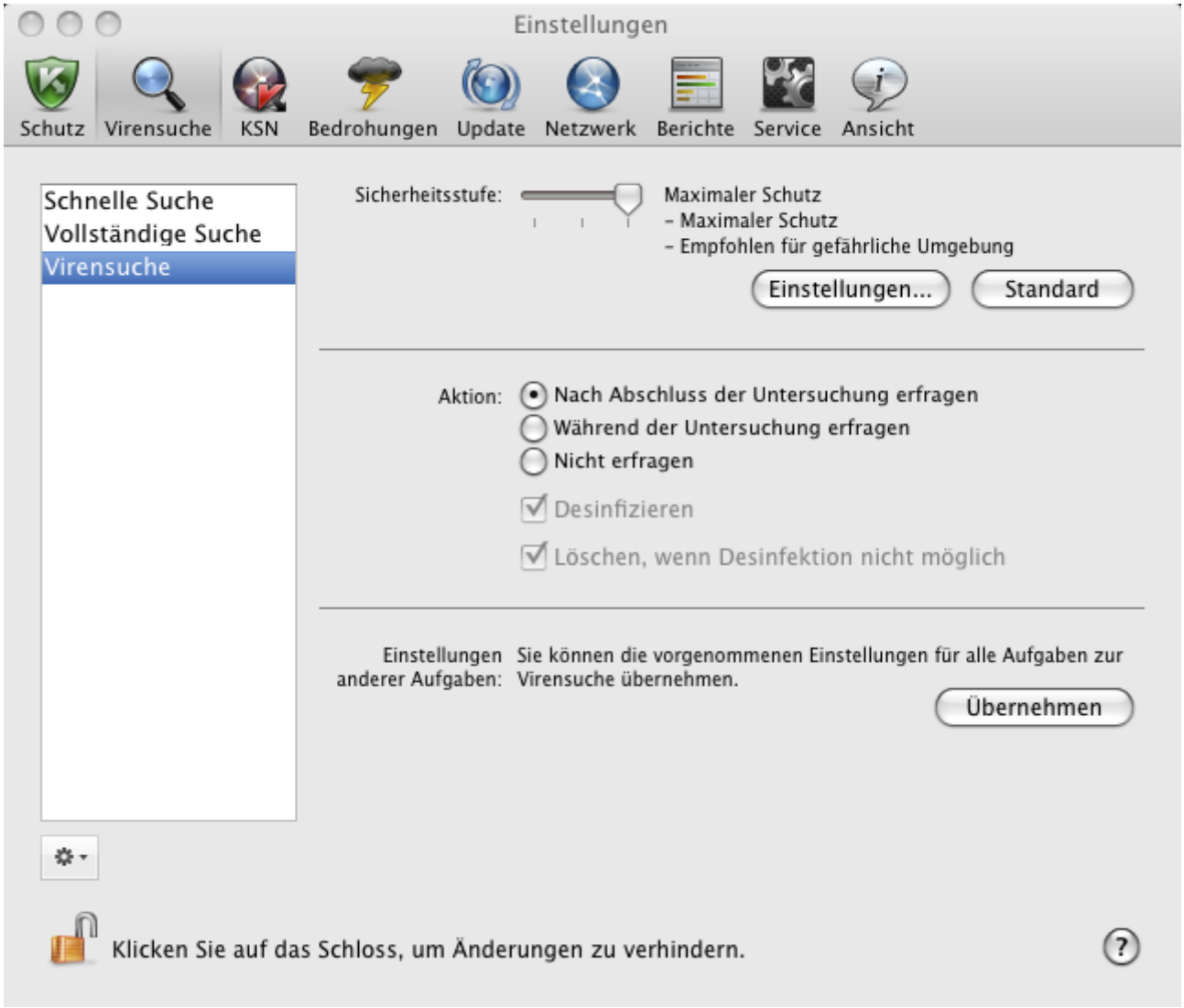

Abbildung 40. Programmkonfigurationsfenster. Aufgabe Virensuche

STATISTIK ÜBER DIE VIRENSUCHE

Kurze Informationen zur Ausführung jeder Untersuchungsaufgabe (mit Prozentangabe) werden im Programmhauptfenster (siehe Abschnitt "Programmhauptfenster" auf Seite 34) angezeigt.

Außerdem wird in Kaspersky Anti-Virus ein Detailbericht über die Ausführung der Untersuchungsaufgaben erstellt.

Um den Bericht über die Ausführung der laufenden Aufgabe zu sehen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Programmhauptfenster (siehe Seite 34), und klicken Sie auf die Schaltfläche .

2. Wählen Sie im Abschnitt **Auszuführende Aufgaben** des folgenden Berichtsfensters den Namen der erforderlichen Aufgabe aus.

Wenn die Untersuchungsaufgabe bereits abgeschlossen ist, werden die Ergebnisse der Aufgabenausführung im Abschnitt **Abgeschlossene Aufgaben** angezeigt.

Im unteren Teil des Berichtsfensters werden Informationen über die Ausführung der laufenden Aufgabe oder die Gesamtstatistik mit den Ergebnissen der abgeschlossenen Untersuchungsaufgabe angezeigt. Die Statistik enthält Angaben über die Anzahl der überprüften Objekte, über die Anzahl gefundener schädlicher Objekte und der Objekte, die eine Bearbeitung erfordern. Außerdem werden hier Informationen über den Startzeitpunkt und das voraussichtliche Ende der Untersuchung sowie die Untersuchungsdauer angezeigt.

Wenn aufgrund der Ausführung einer Aufgabe ein Fehler auftritt, starten Sie die Aufgabe neu. Wenn ein wiederholter Versuch, eine Prüfung durchzuführen auch mit einem Fehler abgeschlossen wird, wenden Sie sich an den Technischen Support von Kaspersky Lab (siehe Abschnitt "Kontaktaufnahme mit dem Technischen Support" auf Seite 113).

Ausführliche Informationen über die Ausführung der Aufgaben zur Virensuche wird rechts im Berichtsfenster auf folgenden Registerkarten vorgestellt:

- Auf der Registerkarte **Gefunden** werden alle gefährlichen Objekte aufgezählt, die im Vorgang der Aufgabenausführung gefunden wurden. Für jedes Objekt sind der Name, der Pfad zu dem Ordner, in dem das Objekt gespeichert wird, sowie der Status angegeben, der ihm von Kaspersky Anti-Virus zugewiesen wurde. Wenn genau festgestellt werden konnte, von welcher Malware das Objekt befallen ist, wird der entsprechende Status vergeben (z.B. *Virus*, *Trojanisches Programm* usw). Wenn der Malware-Typ nicht genau festgestellt werden konnte, erhält das Objekt den Status "*möglicherweise infiziert*". Neben dem Status wird außerdem die Aktion genannt, die mit dem Objekt ausgeführt wurde (*gefunden*, *nicht gefunden*, desinfiziert).

- Auf der Registerkarte **Ereignisse** wird eine vollständige Liste mit Ereignissen geführt, die im Laufe der Ausführung von Aufgaben zur Virensuche entstanden sind, mit Angaben der Zeit des Ereignisses, seiner Bezeichnung, Status und der Entstehungsursache. Die Ereignisse können folgende Status aufweisen:

  - Informatives Ereignis (z.B. *Objekt wurde nicht verarbeitet: nach Typ übersprungen*)

  - Warnung (z.B. *Virus gefunden*)

  - Hinweis (z.B. *Archiv ist kennwortgeschützt*).

- Auf der Registerkarte **Statistik** wird die Gesamtzahl der untersuchten Objekte angezeigt. Einzelne Spalten enthalten Informationen darüber, wie viele Archive und gefährliche Objekte sich unter den untersuchten Objekten befinden, wie viele Objekte desinfiziert oder in die Quarantäne verschoben sind usw.

- Auf der Registerkarte **Einstellungen** werden die wichtigsten Einstellungen angezeigt, mit denen die Aufgabe zur Virensuche ausgeführt wird. Um schnell zur Konfiguration der Sucheinstellungen zu wechseln, klicken Sie auf die Schaltfläche **Einstellungen ändern**.

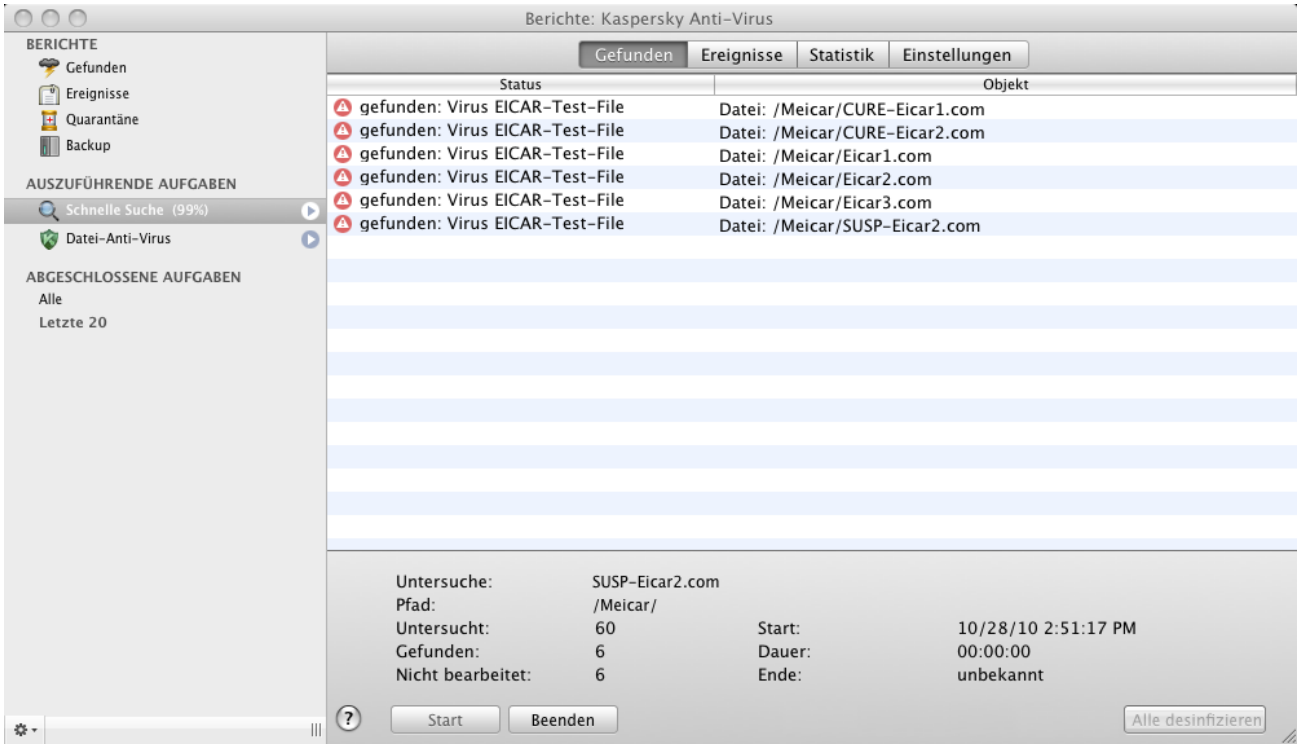

Abbildung 41. Berichtsfenster. Virensuche

PROGRAMM-UPDATE

Die Instandhaltung der Anti-Viren-Datenbanken im aktuellen Zustand bietet Gewähr für die Sicherheit Ihres Computers. Jeden Tag tauchen neue Viren, trojanische und andere schädliche Programme auf. Deshalb ist es sehr wichtig sicherzustellen, dass Ihre Informationen zuverlässig geschützt werden.

Die Aktualisierung von Kaspersky Anti-Virus umfasst den Download und die Installation folgender Elemente auf Ihrem Computer:

- **Anti-Viren-Datenbanken des Programms**

  Der Informationsschutz auf dem Computer wird mit Hilfe der Anti-Viren-Datenbanken gewährleistet. Datei-Anti-Virus (auf Seite 56) und Untersuchungsaufgaben (siehe Abschnitt "Virensuche" auf Seite 68) verwenden diese für die Suche und Neutralisierung schädlicher Objekte auf Ihrem Computer. Die Anti-Viren-Datenbanken werden stündlich mit Einträgen über neue Bedrohungen und Methoden des Kampfes gegen sie aufgefüllt, deshalb wird ausdrücklich empfohlen, diese regelmäßig zu aktualisieren.

- **Programm-Module**

  Neben den Datenbanken können Sie auch die Programm-Module von Kaspersky Anti-Virus aktualisieren. Kaspersky Lab gibt regelmäßig Updatepakete heraus.

Als standardmäßige Updatequelle für Kaspersky Anti-Virus dienen die Kaspersky-Lab-Updateserver.

Um die Updates von den Servern herunterzuladen, ist eine Verbindung Ihres Computers mit dem Internet erforderlich. Wenn die Internetverbindung über einen Proxyserver erfolgt, passen Sie die Netzwerkeinstellungen an (siehe Abschnitt "Proxyserver-Einstellungen anpassen" auf Seite 91).

Wenn Sie keinen Zugang zu den Updateservern von Kaspersky Lab haben (zum Beispiel, Sie haben keinen Internetzugang), wenden Sie sich an den Technischen Support des Kaspersky Lab (siehe Abschnitt "Kontaktaufnahme

mit dem technischen Support" auf Seite 113) für den Erhalt der Updates von Kaspersky Anti-Virus auf CDs im ZIP-Format.

Für den Download von Updates stehen folgende Modi zur Auswahl:

- *Automatisch*: Kaspersky Anti-Virus prüft regelmäßig die Updatequelle auf das Vorhandensein eines Updatepakets . Die Häufigkeit der Überprüfung kann während Viren-Epidemien steigen und unter gewöhnlichen Umständen sinken. Wenn neue Updates vorhanden sind, lädt sie Kaspersky Anti-Virus im Hintergrund herunter und installiert sie auf dem Computer. Dieser Modus wird standardmäßig verwendet.

- *Nach Zeitplan*: Das Update von Kaspersky Anti-Virus wird automatisch, entsprechend dem festgesetztem Zeitplan durchgeführt.

- *Manuell*: In diesem Fall starten Sie die Aktualisierung von Kaspersky Anti-Virus manuell.

Während des Updates werden die Programm-Module und Antiviren-Datenbanken auf Ihrem Computer mit den momentan in der Updatequelle verfügbaren verglichen. Wenn auf Ihrem Computer die aktuelle Version der Datenbanken und Module installiert ist, erscheint im unteren Teil des Programmhauptfensters (siehe Abschnitt "Programmhauptfenster" auf Seite 34) ein Ereignis darüber, dass sich die Anti-Viren-Datenbanken im aktuellen Zustand befinden. Wenn sich die Datenbanken und Module von den momentan in der Updatequelle verfügbaren unterscheiden, wird auf Ihrem Computer nur der fehlende Teil der Updates installiert. Die Datenbanken und Module werden nicht vollständig kopiert, was erlaubt, die Update-Geschwindigkeit zu erhöhen und das Volumen des Netzverkehrs zu reduzieren.

Vor dem Update der Datenbanken und Module erstellt Kaspersky Anti-Virus ihre Sicherheitskopie für den Fall, falls die Notwendigkeit aufkommt, zur Verwendung der vorherigen Version zurück zu kehren. Die Möglichkeit von Rollback (siehe Abschnitt "Rollback vom letzten Update" auf Seite 85) ist hilfreich, zum Beispiel in dem Fall, wenn die neue Version der Datenbanken eine falsche Signatur enthält, wegen der Kaspersky Anti-Virus die sichere Datei blockiert.

Wenn die Datenbanken von Kaspersky Anti-Virus beschädigt sind, wird empfohlen, die Updateaufgabe zu starten, um funktionsfähige aktuelle Datenbanken herunterzuladen.

Gleichzeitig mit dem Update von Kaspersky Anti-Virus kann man die kopierten Updates auf eine lokale Quelle kopieren (siehe Abschnitt "Update von einer lokalen Quelle" auf Seite 86). Dieses Service erlaubt es, die Antiviren-Datenbanken von Kaspersky Anti-Virus und die vom Programm verwendeten Module auf anderen Computern zur Reduzierung des Datenverkehrs lokal zu aktualisieren.

IN DIESEM ABSCHNITT

Update starten 84

Rollback zum vorherigen Update 85

Update von einer lokalen Quelle 86

Update anpassen 87

Statistik für das Update 91

UPDATE STARTEN

Ein rechtzeitiges Update von Kaspersky Anti-Virus erlaubt es, den Schutz des Computers auf dem erforderlichen Stand zu halten. Wenn kein Update der Anti-Viren-Datenbanken und Programm-Module erfolgt, sind die Informationen auf Ihrem Computer ernsthaft gefährdet.

Im unteren Teil des Programmhauptfensters (siehe Abschnitt "Programmhauptfenster" auf Seite 34) werden folgende Informationen zum Update von Kaspersky Anti-Virus vorgestellt: Herstellungsdatum der Anti-Viren-Datenbanken, Anzahl der Einträge, die die auf Ihrem Computer installierten Datenbanken enthalten, sowie Angaben über die Aktualität der

verwendeten Datenbanken. Die Anzahl der Einträge in den Datenbanken spiegelt die Anzahl der momentan bekannten Bedrohungen wider, vor denen der Computer geschützt ist.

Während der Arbeit mit Kaspersky Anti-Virus können Sie jederzeit ein Programmupdate starten. Klicken Sie dazu im Hauptfenster auf die Schaltfläche . Ausführlichere Informationen zur Ausführung dieser Aufgabe werden im Berichtsfenster vorgestellt (siehe Abschnitt "Berichte" auf Seite 98).

Gleichzeitig mit dem Erhalt der Updates von den Servern von Kaspersky Lab wird deren Kopierung auf einer lokalen Quelle durchgeführt (siehe Abschnitt "Update von einer lokalen Quelle" auf Seite 86), unter der Bedingung, dieses Service aktiviert ist.

ROLLBACK ZUM VORHERIGEN UPDATE

Bei jedem Starten des Updates erstellt Kaspersky Anti-Virus zuerst eine Sicherungskopie der bisher verwendeten Datenbanken und Programm-Module und beginnt erst danach mit der Aktualisierung. Diese Arbeitsordnung erlaubt es Ihnen, zur Verwendung der vorherigen Version zurück zu kehren. Die Rollback-Funktion ist beispielsweise nützlich, wenn die neue Datenbankversion eine fehlerhafte Signatur enthält, die dazu führt, dass Kaspersky Anti-Virus ein harmloses Programm blockiert.

Wenn die Datenbanken von Kaspersky Anti-Virus beschädigt sind, wird empfohlen, die Updateaufgabe zu starten, um funktionsfähige aktuelle Datenbanken herunterzuladen.

- *Um zur Verwendung der vorherigen Version der Antiviren-Datenbanken zurückzukehren, gehen Sie folgendermaßen vor:*

1. Öffnen Sie das Programmkonfigurationsfenster (siehe Seite 35), und wählen Sie die Registerkarte **Update** (siehe Abbildung unten) aus.

2. Klicken Sie im Block **Rollback** auf die Schaltfläche **Rollback**.

Die Ergebnisse der Rollback-Ausführung können Sie im Berichtsfenster sehen (siehe Abschnitt "Statistik für das Update" auf Seite 91).

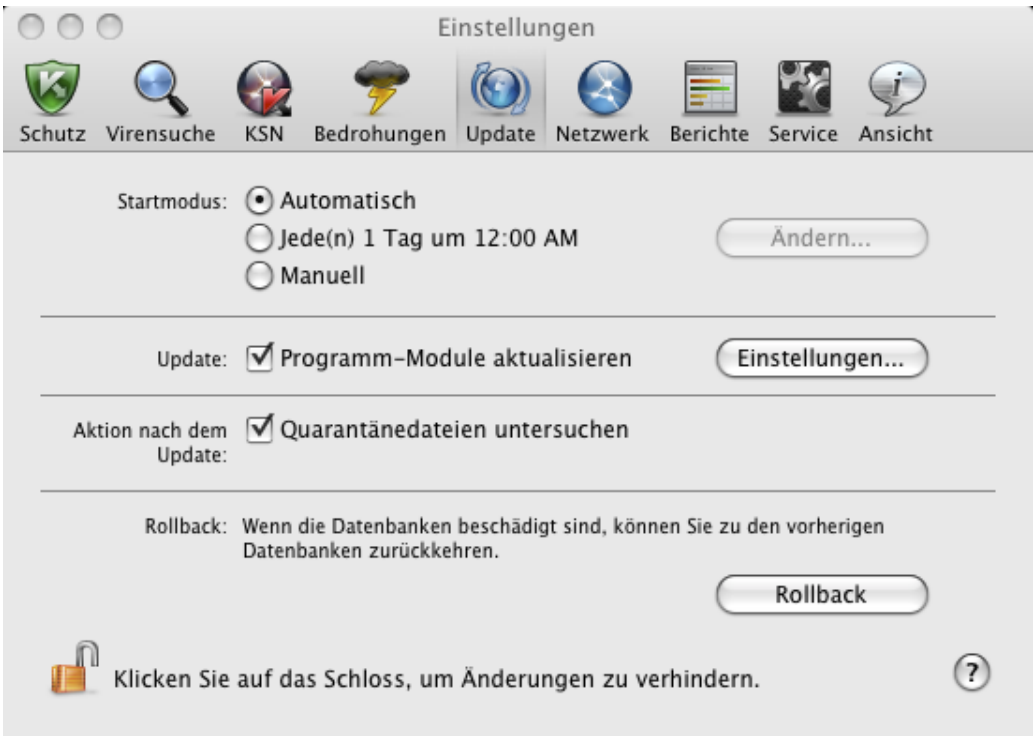

Abbildung 42. Programmkonfigurationsfenster. Update

UPDATE VON EINER LOKALEN QUELLE

Wenn mehrere Computer in einem lokalen Netz verbunden sind, ist es nicht erforderlich die Updates von Kaspersky Anti-Virus für jeden von ihnen getrennt zu erhalten, weil sich in diesem Fall der Netzverkehr deutlich erhöht. Sie können das Kopierservice der erhaltenen Updates nutzen, was Ihnen erlaubt, die Antiviren-Datenbanken von Kaspersky Anti-Virus und die vom Programm verwendeten Module auf anderen Computern lokal zu aktualisieren und somit den Datenverkehr zu reduzieren. Der Update-Download wird auf folgende Weise organisiert:

1. Ein Computer des Netzwerks lädt das Updatepaket für Kaspersky Anti-Virus von den Kaspersky-Lab-Updateservern im Internet oder von einer anderen Webressource herunter, auf der sich die aktuellen Updates befinden. Die heruntergeladenen Updates werden in einem gemeinsamen Ordner abgelegt.

   Der gemeinsame Ordner soll vorher erstellt werden.

2. Andere Netzwerkcomputer wenden sich zum Download der Updates an den gemeinsamen Ordner als zur Updatequelle.

➧ *Um das Kopierservice der Updates in der lokalen Quelle zu aktivieren, gehen Sie folgendermaßen vor:*

1. Öffnen Sie das Programmkonfigurationsfenster (siehe Seite 35), und wählen Sie die Registerkarte **Update** (siehe Abbildung unten) aus.

2. Klicken Sie im Block **Update** auf die Schaltfläche **Einstellungen**.

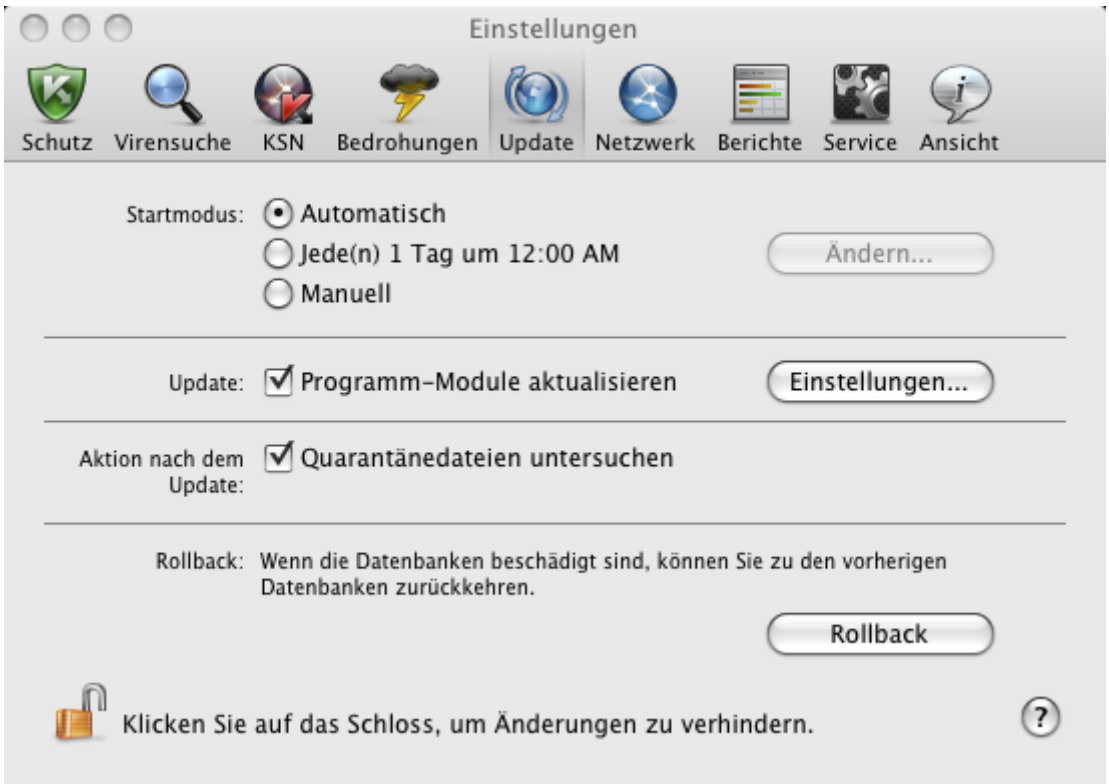

Abbildung 43. Programmkonfigurationsfenster. Update

3. Wählen Sie im folgenden Fenster die Registerkarte **Erweitert** (siehe Abbildung unten) aus. Aktivieren Sie das Kontrollkästchen **Kopieren in den Ordner**, und klicken Sie auf die Schaltfläche **Wählen**.

4. Wählen Sie im folgenden Standardfenster den gemeinsamen Ordner aus, in dem die heruntergeladenen Updates gespeichert werden sollen.

Beachten Sie, dass Kaspersky Anti-Virus von den Kaspersky-Lab-Updateservern nur das für dieses Produkt passende Updatepaket erhält.

Abbildung 44. Update-Verteilung anpassen

UPDATE ANPASSEN

Die Updates von Kaspersky Anti-Virus erfolgen mit folgenden Einstellungen:

- **Startmodus**

  Der Updatemodus legt fest, auf welche Weise die Aktualisierung gestartet werden soll: automatisch (dieser Modus wird von den Spezialisten des Kaspersky Lab empfohlen), manuell oder nach Zeitplan. Bei der Auswahl der letzten Variante muss man einen Zeitplan für den Start der Updateaufgabe erstellen (siehe Abschnitt "Zeitplan für den Start der Updateaufgabe anpassen" auf Seite 90).

- **Updateobjekt**

  Das Updateobjekt bestimmt, was genau aktualisiert wird: nur die Antiviren-Datenbanken oder die Datenbanken und Programm-Module. Die Datenbanken von Kaspersky Anti-Virus werden immer aktualisiert, die Programm-Module nur dann, wenn das entsprechende Kontrollkästchen aktiviert ist (siehe Abschnitt "Updatemodus und Updateobjekt auswählen" auf Seite 88).

- **Updatequelle**

  Die Updatequelle – ist eine Ressource, die aktuelle Dateien der Antiviren-Datenbanken und Module von Kaspersky Anti-Virus enthält. Als Updatequelle können HTTP- oder FTP-Server, lokale Ordner oder Netzwerkordner dienen.

- **Verbindungseinstellungen**

  Für einen erfolgreichen Download von Updates von den Update-Servern von Kaspersky Lab oder anderen Update-Quellen, außer den Lokal- und Netzwerkordnern, ist ein Internetanschluss des Computers erforderlich. Wenn die Internetverbindung über einen Proxyserver erfolgt, passen Sie die Netzwerkeinstellungen an (siehe Abschnitt "Proxyserver-Einstellungen anpassen" auf Seite 91).

UPDATEMODUS UND UPDATEOBJEKT AUSWÄHLEN

Wenn man die Update-Einstellungen von Kaspersky Anti-Virus anpasst, ist es wichtig, das Updateobjekt und den Update-Startmodus festzulegen.

Gehen Sie folgendermaßen vor, um den Startmodus für die Updateaufgabe auszuwählen:

1. Öffnen Sie das Programmkonfigurationsfenster (auf Seite 35), und wählen Sie die Registerkarte **Update** aus (siehe Abbildung unten).

2. Wählen Sie im Block **Startmodus** den Startmodus für die Updateaufgabe aus.

Damit sich während des Update-Vorgangs des Programms auf dem Computer nicht nur die Antiviren-Datenbanken, sondern auch Programm-Module kopiert und installiert werden, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Programmkonfigurationsfenster (auf Seite 35), und wählen Sie die Registerkarte **Update** aus (siehe Abbildung unten).

2. Aktivieren Sie im Block **Update** das Kontrollkästchen **Programm-Module aktualisieren**.

Wenn während der Ausführung der Update-Aufgabe in der Updatequelle auch Updates für Programm-Module erhältlich sind, erhält Kaspersky Anti-Virus diese und setzt sie nach dem Neustart des Computers ein. Die heruntergeladenen Updates für Module werden nicht erst nach dem Neustart installiert. Steht die nächste Aktualisierung des Programms zur Verfügung, bevor der Computer neu gestartet und die zuvor heruntergeladenen Updates der Programm-Module installiert wurden, dann werden nur die Bedrohungssignaturen aktualisiert.

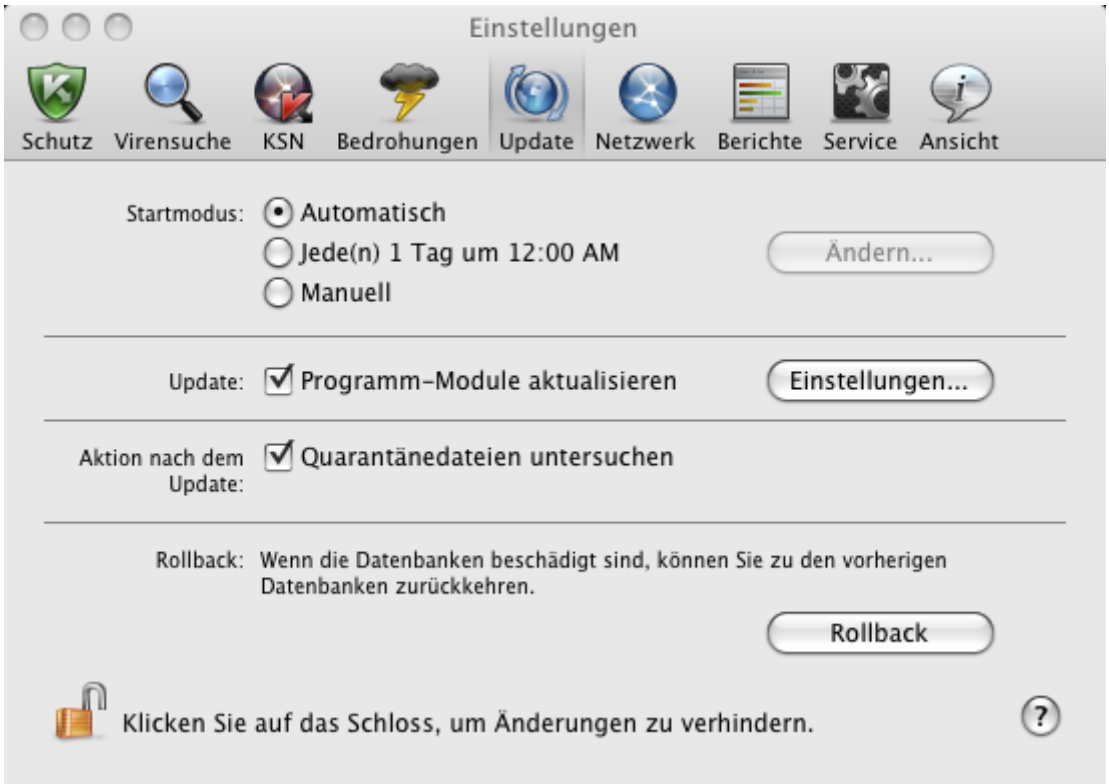

Abbildung 45. Programmkonfigurationsfenster. Update

UPDATEQUELLE AUSWÄHLEN

Eine *Updatequelle* ist eine Ressource, die Updates für die Datenbanken und Module von Kaspersky Anti-Virus enthält. Als Updatequelle können HTTP- oder FTP-Server, lokale Ordner oder Netzwerkordner dienen.

Als primäre Updatequelle des Programms dienen die Updateserver von Kaspersky Lab. Dies sind spezielle Internetseiten, auf denen Updates der Antiviren-Datenbanken und Programm-Module für alle Kaspersky-Lab-Produkte zur Verfügung stehen.

Wenn Sie keinen Zugang zu den Updateservern von Kaspersky Lab haben (zum Beispiel, Sie haben keinen Internetzugang), wenden Sie sich an den Technischen Support des Kaspersky Lab für den Erhalt der Updates im ZIP-Format. Die empfangenen Updates können Sie auf einer FTP- oder HTTP-Seite oder in einem lokalen oder Netzwerkordner sichern.

Geben Sie zur Bestellung von Updates auf Wechseldatenträgern unbedingt an, ob Sie Updates für die Module von Kaspersky Anti-Virus erhalten möchten.

Gehen Sie folgendermaßen vor, um eine Updatequelle von Kaspersky Anti-Virus auszuwählen:

1. Öffnen Sie das Programmkonfigurationsfenster (siehe Seite 35), und wählen Sie die Registerkarte **Update** aus.
2. Klicken Sie im Block **Update** auf die Schaltfläche **Einstellungen**.
3. Wählen Sie im folgenden Fenster die Registerkarte **Updatequelle** (siehe Abbildung unten) aus. Bearbeiten Sie die Liste der Updatequellen, wenn es erforderlich ist.

   In der Grundeinstellung enthält die Liste nur die Kaspersky-Lab-Updateserver. Wenn Kaspersky Anti-Virus das Update durchführt, wendet es sich an diese Liste, wählt die in der Reihenfolge erste Serveradresse aus und versucht, ihr Update herunterzuladen. Wenn die Aktualisierung von der gewählten Adresse erfolglos ist, wendet sich das Programm an die nächste Adresse und versucht erneut, die Updates zu empfangen. Dieser Vorgang wird solange fortgesetzt, bis ein Verbindungsversuch erfolgreich abgeschlossen wurde oder bis alle verfügbaren Updateserver aufgerufen wurden. Nächstes Mal wendet sich das Programm für den Erhalt von Updates zuerst an den Server, von dem die Updates das letzte Mal erfolgreich abgerufen wurden.

   Sie können folgende Aktionen ausführen:

   - Eine neue Updatequelle zur Liste hinzufügen.

     Klicken Sie auf die Schaltfläche und wählen Sie aus der folgende Liste eine auf Sie eher zutreffende Variante (**Pfad** – für einen Lokal-oder Netzwerkordner **URL** – für HTTP-oder FTP-Server). Geben Sie im folgenden Fenster den Speicherort der neuen Updatequelle an.

   - Die Updatequelle verändern.

     Wählen Sie die gewünschte Ausnahmeregel in der Liste aus, und klicken Sie auf die Schaltfläche **Ändern**. Nehmen Sie im folgenden Fenster die erforderlichen Änderungen vor.

     Beachten Sie, dass Kaspersky-Lab-Updateserver als Updatequellen dienen, die nicht bearbeitet bzw. gelöscht werden können.

   - Der Erhalt von Updates aus der Quelle vorübergehend deaktivieren.

     Wählen Sie die Updatequelle in der Liste aus, und deaktivieren Sie das Kontrollkästchen daneben. Das Update von Kaspersky Anti-Virus wird von diesem Server so lange nicht ausgeführt, bis das Kontrollkästchen wieder aktiviert wird.

- Die Updatequelle löschen.

  Wählen Sie die Updatequelle in der Liste aus, und klicken Sie auf die Schaltfläche −.

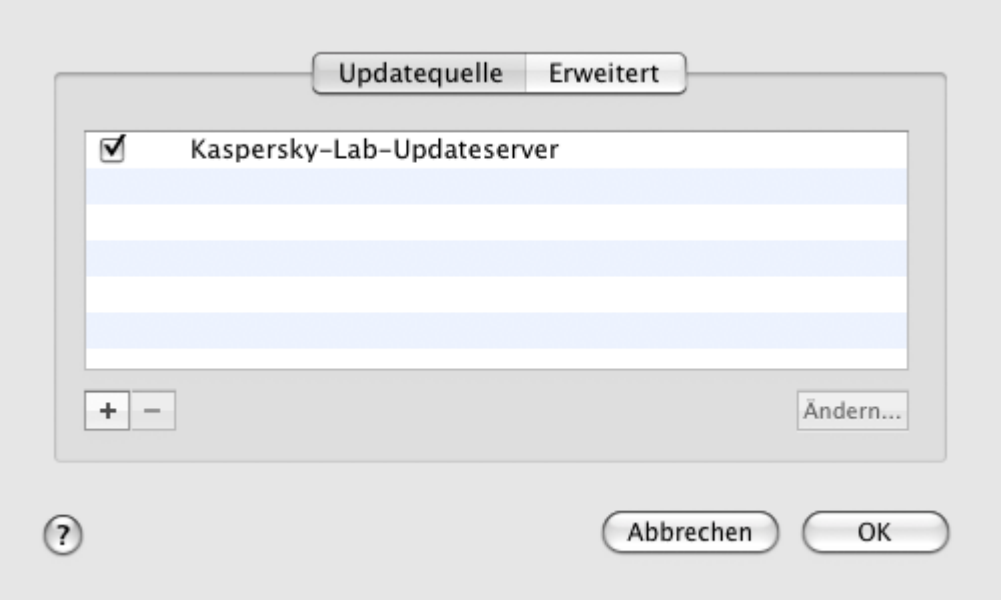

Abbildung 46. Updatequelle auswählen

START DER UPDATEAUFGABEN NACH ZEITPLAN ANPASSEN

Standardmäßig wird Kaspersky Anti-Virus automatisch aktualisiert. Sie können einen anderen Startmodus für die Updateaufgabe auswählen: manuell oder nach einem festgelegten Zeitplan.

Um den zeitgesteuerten Start für die Updateaufgabe von Kaspersky Anti-Virus anzupassen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Programmkonfigurationsfenster (siehe Seite 35), und wählen Sie die Registerkarte **Update** aus.

2. Wählen Sie im Block **Startmodus** die Variante für den Start des Updates nach Zeitplan, und klicken Sie auf die Schaltfläche **Ändern**.

3. Legen Sie im folgenden Fenster (siehe Abbildung unten) die Häufigkeit fest, mit der ein Update des Programms gestartet werden soll.

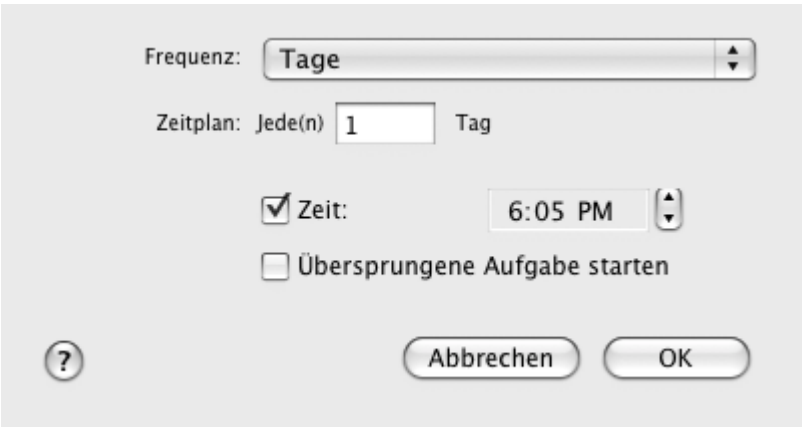

Abbildung 47. Startzeitplan einer Updateaufgabe anpassen

EINSTELLUNGEN FÜR VERBINDUNG MIT PROXY-SERVER

Wenn die Internetverbindung über einen Proxyserver hergestellt wird, passen Sie die Verbindungseinstellungen an. Kaspersky Anti-Virus verwendet diese Einstellungen für das Update der Anti-Viren-Datenbanken und Programm-Module.

Um die Verbindungseinstellungen zum Proxyserver anzupassen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Programmkonfigurationsfenster (siehe Seite 35), und wählen Sie die Registerkarte **Netzwerk** aus (siehe Abbildung unten).

2. Aktivieren Sie im Block **Allgemein** das Kontrollkästchen **Proxyserver verwenden**.

3. Passen Sie im Block **Proxyserver** die Einstellungen des Proxyservers an.

Abbildung 48. Programmkonfigurationsfenster. Netzwerk

Beim Update von einem FTP-Server wird für die Verbindung mit einem Server standardmäßig der passive Modus verwendet. Wenn bei dieser Verbindung ein Fehler auftritt, erfolgt ein Verbindungsversuch im aktiven Modus.

In der Grundeinstellung beträgt der Zeitraum, der für den Verbindungsaufbau mit einem Updateserver zur Verfügung steht, eine Minute. Wenn die Verbindung nicht hergestellt wurde, wird nach Ablauf dieser Frist ein Verbindungsversuch mit der folgenden Updatequelle aus der Liste vorgenommen. Dieser Vorgang wird solange fortgesetzt, bis ein Verbindungsversuch erfolgreich abgeschlossen wurde oder bis alle verfügbaren Updateserver aufgerufen wurden.

STATISTIK FÜR DAS UPDATE

Eine kurze Statistik der laufenden Arbeit des Updateservice (Herstellungsdatum der Antiviren-Datenbanken, Anzahl der Einträge in den Datenbanken und Angaben über die Aktualität der verwendeten Datenbanken) wird im unteren Teil des Programmhauptfensters (siehe Abschnitt "Programmhauptfenster" auf Seite 34).

Wenn noch kein Update von Kaspersky Anti-Virus ausgeführt wurde, fehlt die Angabe des Datums des letzten Updates.

Kaspersky Anti-Virus bietet auch einen ausführlichen Bericht über die Ausführung der der Updateaufgabe an.

Um den Bericht über die Ausführung der laufenden Aufgabe zu sehen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Programmhauptfenster (siehe Seite 34), und klicken Sie auf die Schaltfläche .

2. Wählen Sie im Abschnitt **Auszuführende Aufgaben** des laufenden Fensters die Aufgabe **Update** aus.

Angaben über die Ergebnisse von früheren Updates können Sie im Abschnitt **Abgeschlossene Aufgaben** sehen.

Im unteren Teil des Berichtsfensters werden Informationen über die Ausführung der laufenden Updateaufgabe oder die Gesamtstatistik mit den Ergebnissen des abgeschlossenen Updates angezeigt. Wenn das Update erfolgreich abgeschlossen wurde, enthält die Statistik Angaben über die Höhe der kopierten und installierten Updates, über die Geschwindigkeit, mit der die Updates durchgeführt wurden, über die Start- und Ausführungszeit des Update, sowie über die Dauer der Aufgabenausführung.

Wenn die Operation fehlgeschlagen ist, ist es erforderlich zu prüfen, ob die Update-Einstellungen korrekt sind und ob die Updatequelle verfügbar ist. Starten Sie das Update erneut. Wenn der Versuch wieder fehlerhaft beendet wird, wenden Sie sich an den Technischen Support (siehe Abschnitt "Kontaktaufnahme mit dem technischen Support" auf Seite 113).

Ausführliche Informationen über die Ausführung der Updateaufgabe werden im rechten Teil des Berichtsfensters auf den folgenden Registerkarten angezeigt:

- Auf der Registerkarte **Ereignisse** werden alle Operationen nacheinander aufgeführt, die während des Updatevorgangs durchgeführt wurden. Die Namen der aktualisierten Objekte, die Ordnerpfade, in denen sie gespeichert sind und die Zeiten ihres Abrufs sind ebenfalls angegeben.

- Auf der Registerkarte **Einstellungen** werden die wichtigsten Einstellungen angezeigt, mit denen das Update durchgeführt wurde. Um zur Komponentenkonfiguration zu wechseln, klicken Sie auf die Schaltfläche **Einstellungen ändern**.

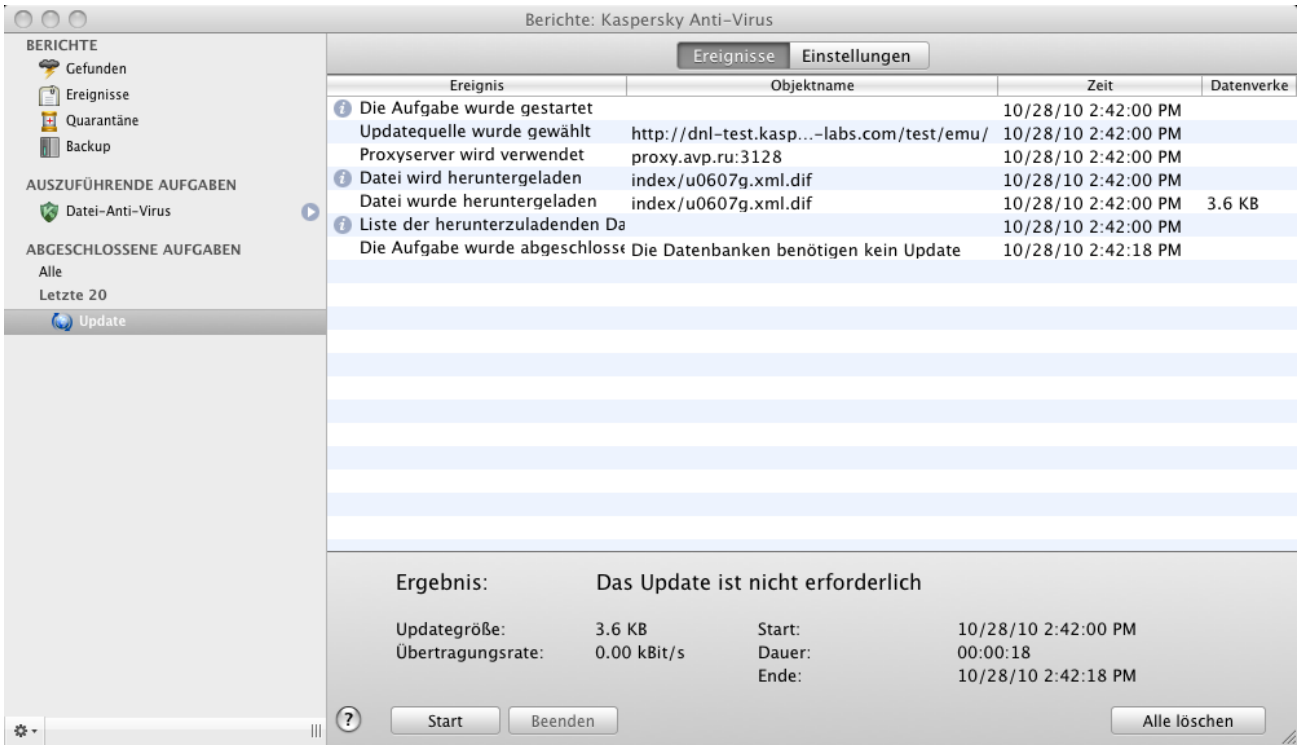

Abbildung 49. Berichtsfenster. Update

BERICHTE UND SPEICHER

Kaspersky Anti-Virus ermöglicht das Sichern von möglicherweise infizierten Objekten in der Quarantäne, Anlegen von Kopien infizierter Objekte vor der Desinfektion oder Löschung im Backup sowie das Erstellen ausführlicher Berichte über die Ausführung jeder Programmkomponente.

IN DIESEM ABSCHNITT

Quarantäne 93

Backup 96

Berichte 98

Berichte und Backups anpassen 100

QUARANTÄNE

Die *Quarantäne* ist ein spezieller Speicher, in den Objekte verschoben werden, die möglicherweise von Viren infiziert sind.

Möglicherweise infizierte Objekte sind Objekte, die verdächtig sind, von Viren oder Virenmodifikationen infiziert zu sein. Der Status *möglicherweise infiziert* kann dem Objekt in den folgenden Fällen vergeben werden:

- Der Code des analysierten Objekts weist Ähnlichkeiten mit einer bekannten Bedrohung auf, wurde aber teilweise verändert.

  Die Antiviren-Datenbanken von Kaspersky Anti-Virus enthalten die Bedrohungen, die momentan von den Spezialisten des Kaspersky Lab. Wenn die Datenbanken noch keine Informationen zur Modifikation eines schädlichen Programms enthalten, zählt Kaspersky Anti-Virus ein Objekt, das durch eine solche Modifikation infiziert ist, zu möglicherweise infizierten Objekten und zeigt an, welcher Bedrohung sich diese Infizierung ähnelt.

- Der Code des gefundenen Objekts erinnert seiner Struktur nach ein schädliches Programm, jedoch enthalten die Datenbanken von Kaspersky Anti-Virus keine ähnlichen Einträge.

  Es ist durchaus möglich, dass es sich um eine neue Art von Bedrohung handelt. Deshalb stuft Kaspersky Anti-Virus das Objekt als möglicherweise infiziert ein.

Ein möglicherweise infiziertes Objekt kann von Datei-Anti-Virus (siehe Abschnitt "Datei-Anti-Virus" auf Seite 56) sowie bei der Ausführung der Untersuchungsaufgaben (siehe Abschnitt "Virensuche" auf Seite 68) entdeckt und in die Quarantäne verschoben werden.

Außerdem können Sie das Objekt manuell in die Quarantäne verschieben, indem Sie auf die Schaltfläche **Quarantäne** in der speziellen Anzeige klicken (siehe Abschnitt "Was tun beim Erscheinen von Programmanzeigen" auf Seite 51), die auf dem Bildschirm Ihres Computers beim Fund eines möglicherweise infizierten Objekts erscheint.

Wenn Sie ein möglicherweise infiziertes Objekt in die Quarantäne verschieben, löscht Kaspersky Anti-Virus es aus dem aktuellen Ordner und speichert es im Quarantäne-Ordner. Die unter Quarantäne stehenden Dateien werden in einem speziellen Format gespeichert und stellen keine Gefahr für die Arbeit des Computers dar.

DEN INHALT DER QUARANTÄNE ANZEIGEN

Der Inhalt der Quarantäne wird im Abschnitt**Quarantäne** des Berichtsfenster angezeigt (siehe Abbildung unten).

Um den Inhalt der Quarantäne anzuzeigen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Programmhauptfenster (siehe Seite 34), und klicken Sie auf die Schaltfläche . Daraufhin wird das Berichtsfenster von Kaspersky Anti-Virus geöffnet.

2. Wählen Sie im linken Bereich des Fensters **Quarantäne** aus. Auf der rechten Seite des Fensters wird der Inhalt des Speichers angezeigt.

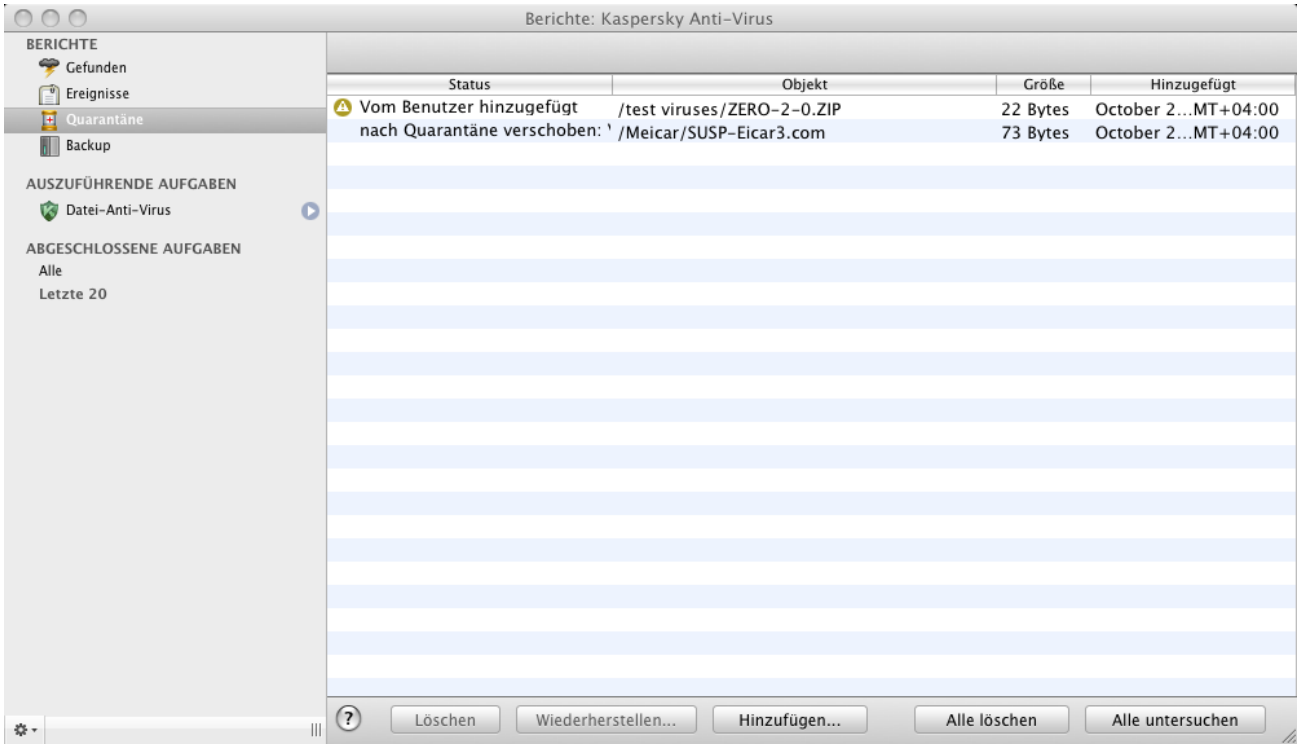

Abbildung 50. Berichtsfenster. Quarantäne

OBJEKTE IN DER QUARANTÄNE

Kaspersky Anti-Virus erlaubt es, folgende Aktionen mit den möglicherweise infizierten Objekten durchzuführen:

- Dateien manuell in die Quarantäne verschieben, bei denen Sie das Vorhandensein eines Virus vermuten, der nicht von Kaspersky Anti-Virus gefunden wurde.

  Klicken Sie dafür im Anzeigefenster der Quarantäne (siehe Abbildung unten) auf die Schaltfläche **Hinzufügen** und wählen Sie im folgenden Standardfenster die benötigte Datei aus. Sie wird mit dem Status *vom Benutzer hinzugefügt* zur Liste hinzugefügt.

- Alle möglicherweise infizierten Quarantäneobjekte untersuchen und desinfizieren unter Verwendung der aktuellen Version der Datenbanken von Kaspersky Anti-Virus.

  Klicken Sie dafür im Anzeigefenster der Quarantäne (siehe Abbildung unten) auf die Schaltfläche **Alles untersuchen**. Aufgrund der Untersuchung und Desinfektion eines Quarantäneobjekts kann sich sein Status in *Fehlalarm* oder *nach Quarantäne verschoben* ändern.

  Standardmäßig untersucht Kaspersky Anti-Virus die Quarantäneobjekte automatisch nach jedem Update (siehe Abschnitt "Quarantäneobjekte nach dem Programmupdate untersuchen" auf Seite 95).

- Dateien in den Ordner, der vom Benutzer festgelegt wurde, oder einen Ordner, in den sie aus der Quarantäne (standardmäßig) verschoben wurden, wiederherstellen.

Um das Objekt wiederherzustellen, wählen Sie es im Anzeigefenster der Quarantäne aus (siehe Abbildung unten) und klicken Sie auf die Schaltfläche **Wiederherstellen**. Bestätigen Sie die Aktion im folgenden Fenster. Bei der Wiederherstellung von Objekten, die aus Archiven, Maildatenbanken und Mail-Format-Dateien in die Quarantäne verschoben wurden, muss zusätzlich der Ordner angegeben werden, in dem sie wiederhergestellt werden sollen.

Es wird empfohlen, nur Objekte mit dem Status *Fehlalarm* wiederherzustellen, weil die Wiederherstellung anderer Objekte zu einer Infektion Ihres Computers führen kann.

- Ein Objekt aus der Quarantäne löschen.

  Löschen Sie nur die Objekte, die nicht desinfiziert werden können. Um ein Objekt zu löschen, wählen Sie es im Anzeigefenster der Quarantäne aus (siehe Abbildung unten) und klicken Sie auf die Schaltfläche **Löschen**. Um den gesamten Inhalt der Quarantäne zu löschen, klicken Sie auf die Schaltfläche **Alle löschen**. Sie können auch die automatische Löschung von älteren Objekten aus der Quarantäne anpassen (siehe Abschnitt "Quarantäne- und Backup-Einstellungen anpassen" auf Seite 101).

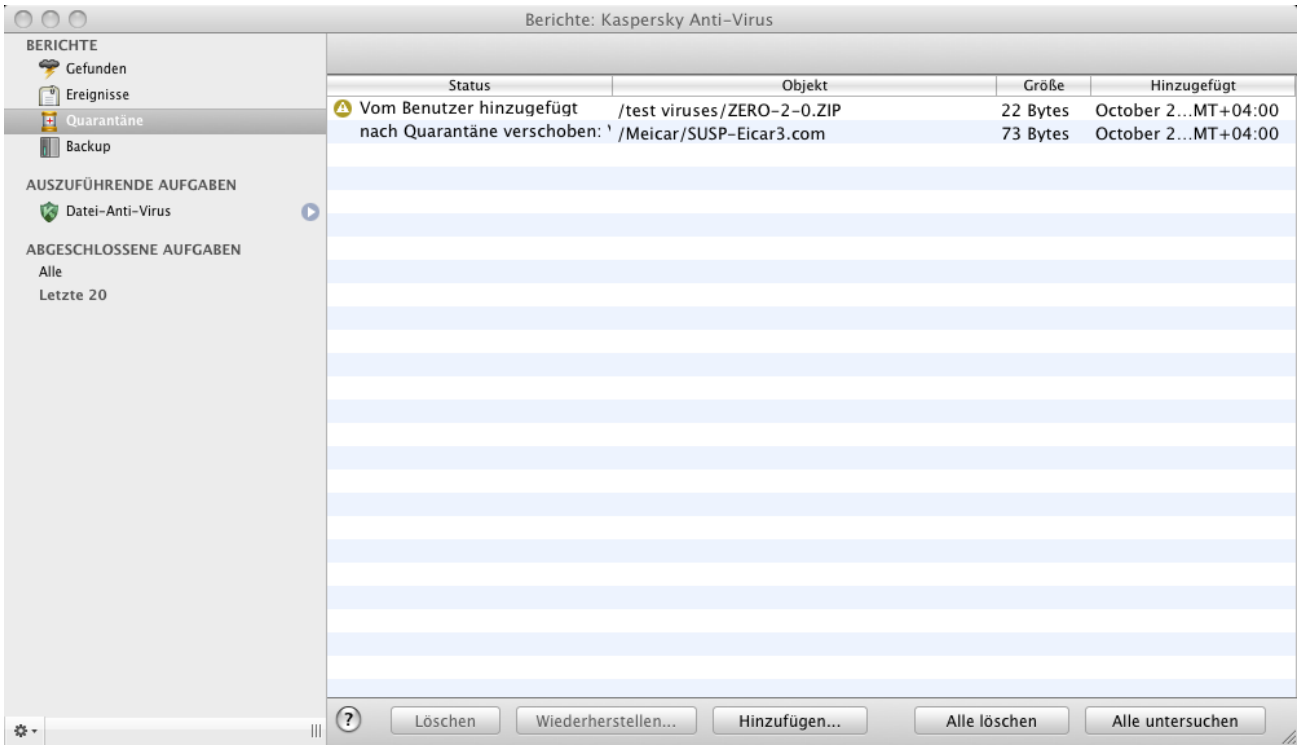

Abbildung 51. Berichtsfenster. Quarantäne

QUARANTÄNEOBJEKTE NACH DEM PROGRAMMUPDATE UNTERSUCHEN

Jedes Updatepaket für die Antiviren-Datenbanken des Programms enthält neue Einträge, die es erlauben, Ihren Computer vor kürzlich entstandenen Bedrohungen zu schützen. Spezialisten von Kaspersky Lab empfehlen Ihnen, sofort nach dem Programmupdate die möglicherweise infizierten Objekte zu untersuchen, die in die Quarantäne verschoben wurden (siehe Abschnitt "Quarantäne" auf Seite 93).

In die Quarantäne werden die Objekte verschoben, bei denen während der Untersuchung durch Datei-Anti-Virus oder der Aufgabeausführung zur Virensuche nicht eindeutig festgestellt werden konnte, durch welche schädlichen Programme sie infiziert wurden. Möglicherweise kann Kaspersky Anti-Virus die Bedrohung eindeutig bestimmen und desinfizieren, nachdem die Datenbanken aktualisiert wurden.

Standardmäßig untersucht Kaspersky Anti-Virus die Quarantäneobjekte nach jedem Update.

Kaspersky Anti-Virus kann die Quarantäneobjekte nicht sofort nach dem Datenbank-Update untersuchen, wenn Sie gerade mit der Quarantäne arbeiten.

Eine Untersuchung des Quarantäne-Inhalts kann nach jedem Programmupdate deaktiviert werden, indem man das entsprechende Kontrollkästchen auf der Registerkarte **Update** im Programmkonfigurationsfenster deaktiviert.

BACKUP

Manchmal gelingt es nicht bei der Desinfektion von infizierten Objekten ihre Unversehrtheit zu sichern. Wenn ein desinfiziertes Objekt wichtige Informationen enthielt, die aufgrund der Desinfektion vollständig oder teilweise verloren gegangen sind, können Sie versuchen, das ursprüngliche Objekt über seine Sicherungskopie wiederherzustellen.

Eine *Sicherungskopie* ist eine Kopie des gefährlichen Originalobjekts. Sie wird bei der ersten Desinfektion oder beim Löschen des Objekts erstellt und im Backup gespeichert.

Backup ist ein spezieller Speicher, der Sicherungskopien von bearbeiteten und gelöschten gefährlichen Objekten enthält. Die Hauptfunktion des Backups besteht in der Möglichkeit, das ursprüngliche Objekt jederzeit wiederherzustellen. Die Sicherungskopien werden im Backup in einem speziellen Format gespeichert und stellen keine Gefahr dar.

DEN INHALT DES BACKUPS ANZEIGEN

Den Inhalt des Backups kann man im Abschnitt **Backup** im Berichtsfenster sehen (siehe Abbildung unten).

➧ *Um den Inhalt des Backups anzuzeigen, gehen Sie folgendermaßen vor:*

1. Öffnen Sie das Programmhauptfenster (siehe Seite 34), und klicken Sie auf die Schaltfläche . Daraufhin wird das Berichtsfenster von Kaspersky Anti-Virus geöffnet.

2. Wählen Sie im linken Bereich des Fensters **Backup** aus. Auf der rechten Seite des Fensters wird der Inhalt des Speichers angezeigt.

   Für jede Kopie werden folgende Informationen angegeben: vollständiger Name des Objekts mit Pfadangabe des ursprünglichen Speicherorts, Zeit seines Verschiebens in den Speicher, Status des Objekts, der ihm aufgrund der Untersuchung zugewiesen wurde, und Größe.

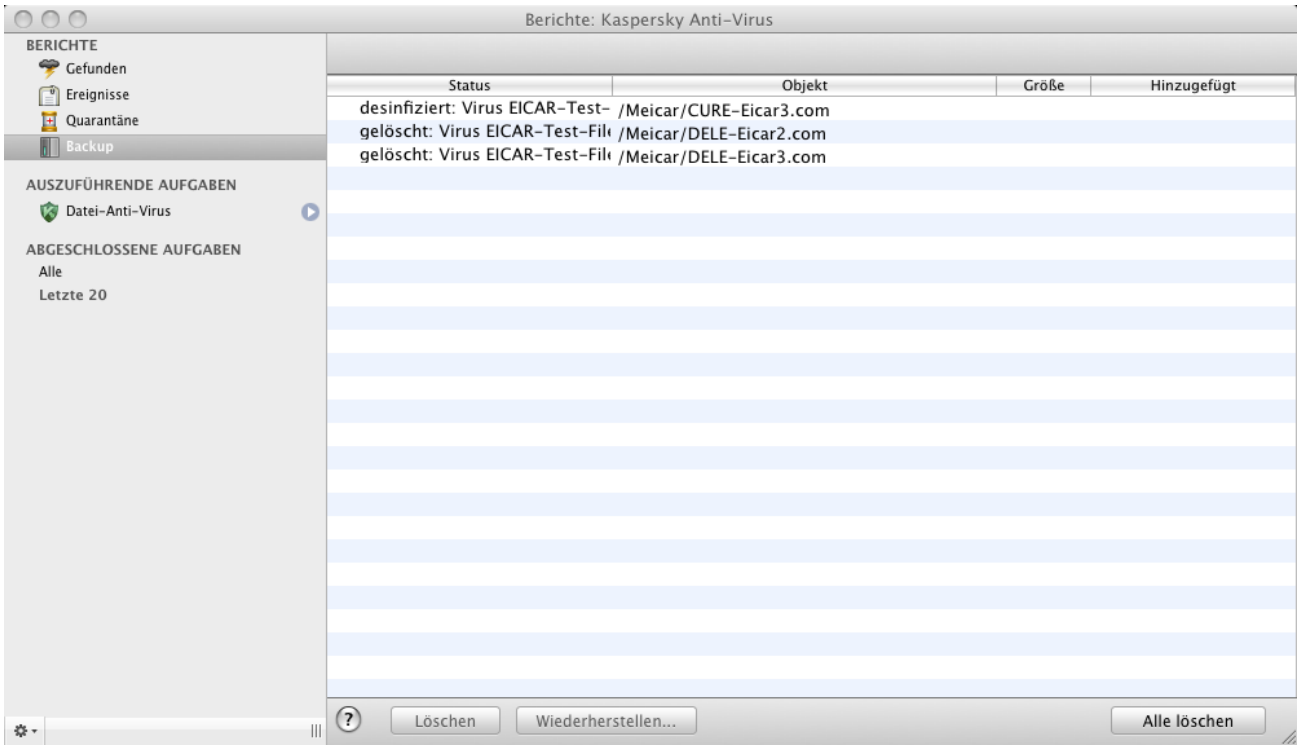

Abbildung 52. Berichtsfenster. Backup

SICHERUNGSKOPIEN VERWENDEN

Kaspersky Anti-Virus erlaubt es, folgende Aktionen mit den Sicherungskopien der Objekte auszuführen:

- Ausgewählte Sicherungskopien aus der Quarantäne wiederherstellen.

  Wählen Sie dafür im Anzeigefenster der Quarantäne (siehe Abbildung unten) eine Sicherungskopie des erforderlichen Objekts in der Liste aus und klicken Sie auf die Schaltfläche **Wiederherstellen**. Bestätigen Sie die Aktion im folgenden Fenster. Das Objekt wird unter dem gleichen Namen am ursprünglichen Speicherort wiederhergestellt, den es vor der Desinfektion trug. Wenn sich am ursprünglichen Speicherort ein Objekt mit dem gleichen Namen befindet (Diese Situation ist möglich, wenn ein Objekt wiederhergestellt wird, dessen Kopie bereits vor der Desinfektion angelegt wurde), erscheint eine entsprechende Warnung auf dem Bildschirm. Sie können den Speicherort des wiederherzustellenden Objekts ändern oder es umbenennen.

  Es wird empfohlen sofort nach der Wiederherstellung das Objekt auf Viren zu untersuchen. Möglicherweise gelingt es, das Objekt mit aktualisierten Datenbanken ohne Datenverlust zu desinfizieren.

  Es wird davor gewarnt, Sicherungskopien von Objekten wiederherzustellen, wenn dies nicht absolut erforderlich ist. Dies kann zu einer Infektion des Computers führen.

- Sicherungskopien aus der Quarantäne löschen.

  Es wird empfohlen die Quarantäne regelmäßig anzusehen und ihre Reinigung durchzuführen. Um Objekte zu löschen, wählen Sie diese im Anzeigefenster der Quarantäne aus (siehe Abbildung unten) und klicken Sie auf die Schaltfläche **Löschen**. Um den gesamten Inhalt des Backups zu löschen, klicken Sie auf die Schaltfläche **Alle löschen**. Sie können auch die Löschung von älteren Sicherungskopien aus der Quarantäne anpassen (siehe Abschnitt "Quarantäne- und Backup-Einstellungen anpassen" auf Seite 101).

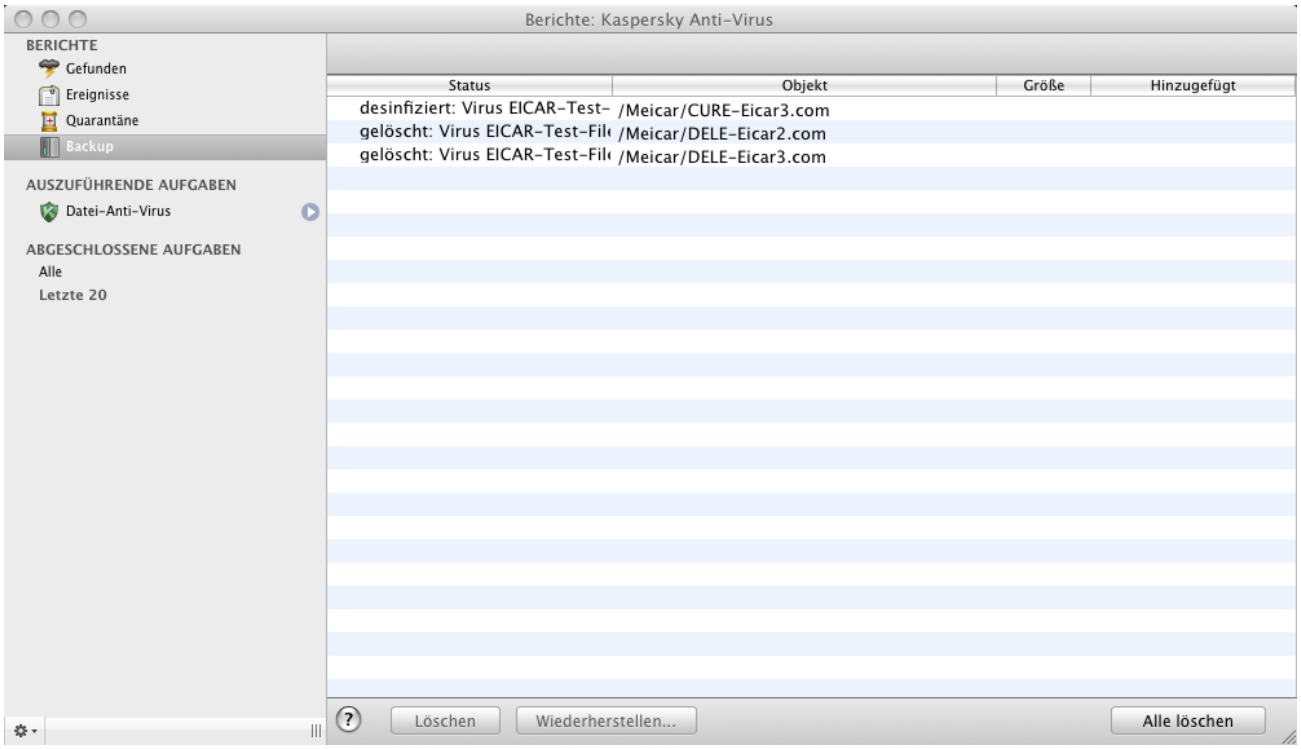

Abbildung 53. Berichtsfenster. Backup

BERICHTE

Kaspersky Anti-Virus bietet die Möglichkeit an, einen ausführlichen Bericht über die Ergebnisse seiner allgemeinen Arbeit mit der Auflistung aller Ereignisse zu erhalten, die in der Programmarbeit entstanden sind. Außerdem wird ein ausführlicher Bericht für jede Programmkomponente getrennt formiert: Datei-Anti-Virus (siehe Abschnitt "Statistik des Dateischutzes" auf Seite 66), Aufgaben zur Virensuche (siehe Abschnitt "Statistik der Virensuche" auf Seite 81) und Updates (siehe Abschnitt "Update-Statistik" auf Seite 91).

Um das Berichtsfenster zu öffnen,

öffnen Sie das Programmhauptfenster (siehe Seite 34), und klicken Sie auf die Schaltfläche .

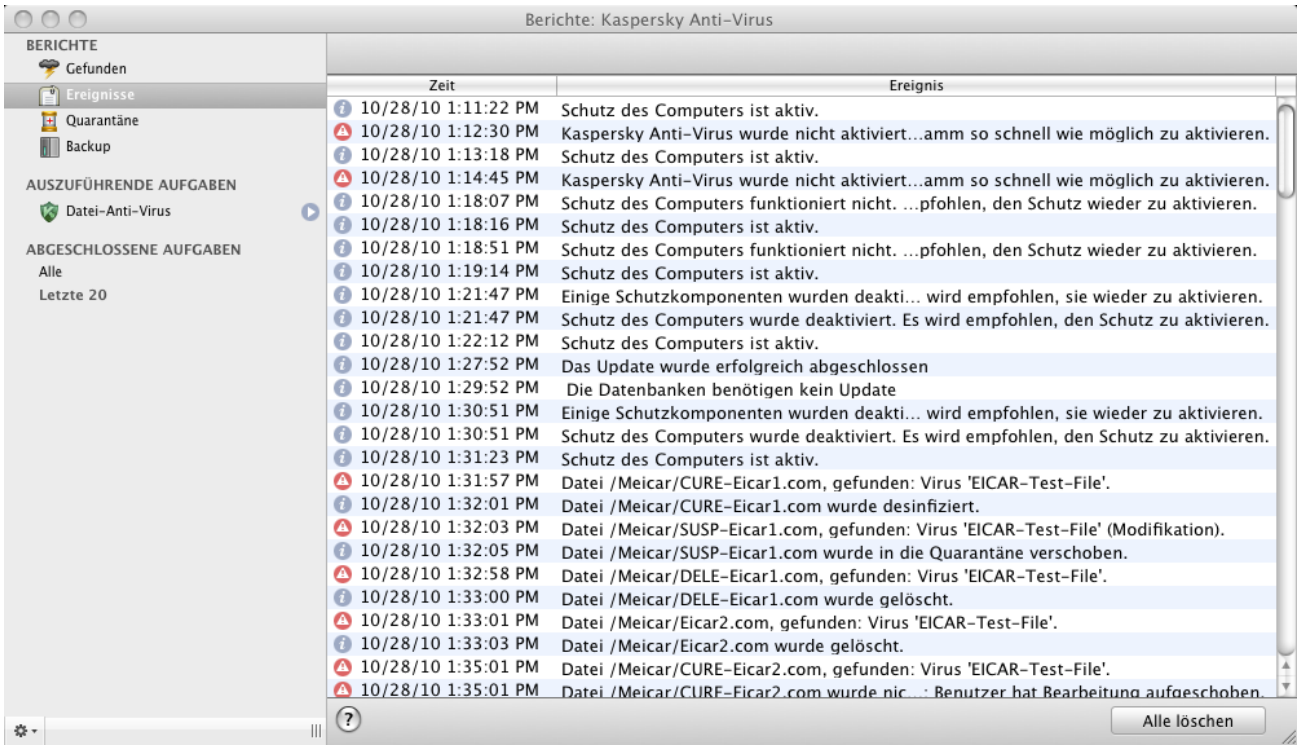
Berichte: Kaspersky Anti-Virus
BERICHTE
Gefunden
Ereignisse
Quarantäne
Backup
AUSZUFÜHRENDE AUFGABEN
Datei-Anti-Virus
ABGESCHLOSSENE AUFGABEN
Alle
Letzte 20
Zeit
Ereignis
10/28/10 1:11:22 PM Schutz des Computers ist aktiv.
10/28/10 1:12:30 PM Kaspersky Anti-Virus wurde nicht aktiviert...amm so schnell wie möglich zu aktivieren.
10/28/10 1:13:18 PM Schutz des Computers ist aktiv.
10/28/10 1:14:45 PM Kaspersky Anti-Virus wurde nicht aktiviert...amm so schnell wie möglich zu aktivieren.
10/28/10 1:18:07 PM Schutz des Computers funktioniert nicht. ...pfohlen, den Schutz wieder zu aktivieren.
10/28/10 1:18:16 PM Schutz des Computers ist aktiv.
10/28/10 1:18:51 PM Schutz des Computers funktioniert nicht. ...pfohlen, den Schutz wieder zu aktivieren.
10/28/10 1:19:14 PM Schutz des Computers ist aktiv.
10/28/10 1:21:47 PM Einige Schutzkomponenten wurden deakti... wird empfohlen, sie wieder zu aktivieren.
10/28/10 1:21:47 PM Schutz des Computers wurde deaktiviert. Es wird empfohlen, den Schutz zu aktivieren.
10/28/10 1:22:12 PM Schutz des Computers ist aktiv.
10/28/10 1:27:52 PM Das Update wurde erfolgreich abgeschlossen
10/28/10 1:29:52 PM Die Datenbanken benötigen kein Update
10/28/10 1:30:51 PM Einige Schutzkomponenten wurden deakti... wird empfohlen, sie wieder zu aktivieren.
10/28/10 1:30:51 PM Schutz des Computers wurde deaktiviert. Es wird empfohlen, den Schutz zu aktivieren.
10/28/10 1:31:23 PM Schutz des Computers ist aktiv.
10/28/10 1:31:57 PM Datei /Meicar/CURE-Eicar1.com, gefunden: Virus 'EICAR-Test-File'.
10/28/10 1:32:01 PM Datei /Meicar/CURE-Eicar1.com wurde desinfiziert.
10/28/10 1:32:03 PM Datei /Meicar/SUSP-Eicar1.com, gefunden: Virus 'EICAR-Test-File' (Modifikation).
10/28/10 1:32:05 PM Datei /Meicar/SUSP-Eicar1.com wurde in die Quarantäne verschoben.
10/28/10 1:32:58 PM Datei /Meicar/DELE-Eicar1.com, gefunden: Virus 'EICAR-Test-File'.
10/28/10 1:33:00 PM Datei /Meicar/DELE-Eicar1.com wurde gelöscht.
10/28/10 1:33:01 PM Datei /Meicar/Eicar2.com, gefunden: Virus 'EICAR-Test-File'.
10/28/10 1:33:03 PM Datei /Meicar/Eicar2.com wurde gelöscht.
10/28/10 1:35:01 PM Datei /Meicar/CURE-Eicar2.com, gefunden: Virus 'EICAR-Test-File'.
10/28/10 1:35:01 PM Datei /Meicar/CURE-Eicar2.com wurde nic... : Benutzer hat Bearbeitung aufgeschoben.
Alle löschen

Abbildung 54. Berichtsfenster von Kaspersky Anti-Virus

Das Berichtsfenster enthält die folgenden Abschnitte:

- **Berichte**: Statistische Angaben zu gefundenen gefährlichen Objekten, Objekten, die in die Quarantäne und ins Backup verschoben wurden, sowie eine Liste mit Ereignissen, die in der Programmarbeit aufgezeichnet wurden. Die Statistiken sind in die folgenden Unterabschnitte unterteilt:

  - **Gefunden**: Liste von allen von Datei-Anti-Virus und Untersuchungsaufgaben gefundenen gefährlichen und verdächtigen Objekten. Um gefährliche Objekte sofort zu desinfizieren, klicken Sie auf die Schaltfläche **Alle desinfizieren**. Um die Berichtseinträge für erkannte Objekte zu löschen, klicken Sie auf die Schaltfläche **Leeren**. Beachten Sie, dass alle gefundenen gefährlichen Objekte dabei auf Ihrem Computer verbleiben.

  - **Ereignisse**: Liste von allen bei der Arbeit von Kaspersky Anti-Virus aufgetretenen Ereignissen. Um die Informationen aus der Liste zu löschen, klicken Sie auf die Schaltfläche **Alle löschen**.

  - **Quarantäne**: Liste der Objekte in der Quarantäne (siehe Abschnitt"Quarantäne" auf Seite 93).

  - **Backup**: Liste der Objekte, die ins Backup verschoben wurden (siehe Seite 96).

- **Auszuführende Aufgaben**: Liste der Aufgaben, die momentan von Kaspersky Anti-Virus ausgeführt werden. Wenn keine Aufgabe gestartet wurde und Datei-Anti-Virus deaktiviert ist, bleibt die Liste leer.

- **Abgeschlossene Aufgaben**: Liste der abgeschlossenen Aufgaben. Sie können alle abgeschlossenen oder die letzten zwanzig Aufgaben nachlesen. Um die Liste zu leeren, klicken Sie in der linken unteren Ecke des Berichtsfensters auf die Schaltfläche und wählen den Befehl **Alle abgeschlossenen Aufgaben löschen** aus.

Über das Berichtsfenster können Sie den Datei-Anti-Virus verwalten sowie die Aufgaben Virensuche und Update starten, beenden und anhalten. Verwenden Sie dafür die gleichnamigen Schaltflächen im Berichtsfenster der konkreten Komponente oder Aufgabe.

Kaspersky Anti-Virus erlaubt es, einen Bericht seiner Arbeit im Textformat zu sichern. Diese Möglichkeit kann in dem Fall gebraucht werden, wenn in der Arbeit mit Datei-Anti-Virus oder bei der Ausführung einer anderen Aufgabe ein Fehler aufgetreten ist, den Sie nicht selbstständig beseitigen können, und die Hilfe des Technischen Supports des Kaspersky

Lab gebraucht wird (siehe Abschnitt "Kontaktaufnahme mit dem technischen Support" auf Seite 113). In diesem Fall soll der Bericht im Textformat an den technischen Support gesendet werden, damit unsere Spezialisten das Problem untersuchen und es möglichst bald lösen können.

Um den Bericht über Kaspersky Anti-Virus in eine Textdatei zu exportieren, gehen Sie folgendermaßen vor:

1. Wählen Sie im Berichtsfenster den erforderlichen Bericht oder Aufgabe aus.

2. Klicken Sie in der linken unteren Ecke des Berichtsfensters auf die Schaltfläche , wählen Sie den Befehl **Exportieren** aus und geben im folgenden Fenster den Dateinamen und den Ordner an, in dem die Datei gespeichert werden soll.

BERICHTE UND BACKUPS ANPASSEN

Auf der Registerkarte **Berichte** des Programmanzeigefensters (siehe Abschnitt "Programmanzeigefenster" auf Seite 35) können Sie das Erstellen und Sichern von Berichten und die maximale Speicherdauer der Objekte in der Quarantäne und im Backup anpassen.

BERICHTSPARAMETER ANPASSEN

Um die Parameter für das Erstellen und Sichern von Berichten anzupassen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Programmkonfigurationsfenster (siehe Seite 35), und wählen Sie die Registerkarte **Berichte** (siehe Abbildung unten) aus.

2. Passen Sie im Block **Berichte** folgende Einstellungen an:

   - Erlauben, dass Ereignisse mit rein informativem Charakter im Bericht aufgezeichnet werden.

     In der Regel sind solche Ereignisse nicht für den Schutz wichtig. Um solche Ereignisse im Bericht zu erfassen, aktivieren Sie das Kontrollkästchen **Informative Ereignisse protokollieren**.

   - Nur wichtige Ereignisse im Bericht zu sichern, die beim letzten Aufgabenstart eingetreten sind.

     Dadurch kann Festplattenplatz gespart werden, weil der Bericht eine geringere Größe aufweist. Wenn das Kontrollkästchen **Nur aktuelle Ereignisse sichern** aktiviert ist, werden die Berichtsdaten bei jedem Neustart der Aufgabe aktualisiert: Wichtige Daten (wie Einträge über erkannte schädliche Objekte) werden gespeichert, unkritische Daten werden gelöscht wurde.

   - Speicherdauer für Berichte festlegen.

     Die maximale Speicherdauer für Objekte beträgt standardmäßig 30 Tage. Danach werden die Objekte gelöscht. Sie können die maximale Speicherdauer ändern oder diese Beschränkung völlig aufheben.

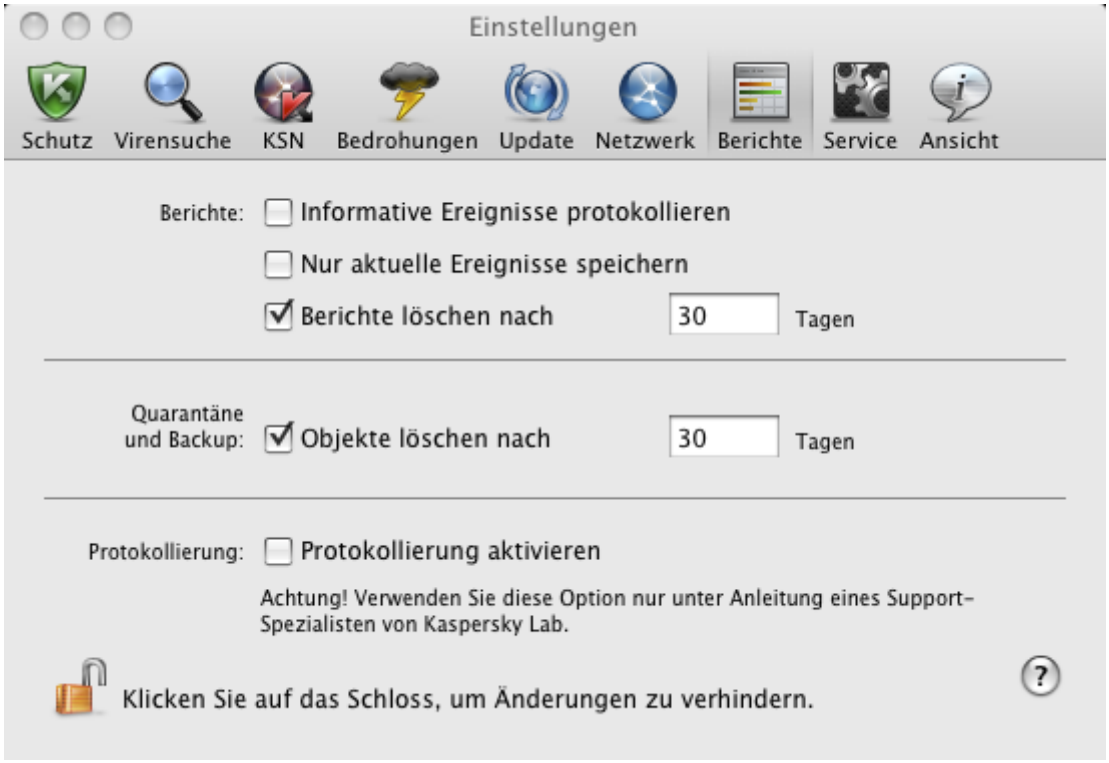

Abbildung 55. Programmkonfigurationsfenster. Berichte

EINSTELLUNGEN FÜR QUARANTÄNE UND BACKUP ANPASSEN

Die Speicherdauer für Quarantäne- und Backup-Objekte beträgt standardmäßig 30 Tage. Danach werden die Objekte gelöscht. Sie können die maximale Speicherdauer der Objekte in der Quarantäne und im Backup ändern oder diese Beschränkung völlig aufheben.

Um die Parameter für das Sichern von Backup-Objekten anzupassen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Programmkonfigurationsfenster (siehe Seite 35), und wählen Sie die Registerkarte **Berichte** (siehe Abbildung unten) aus.

2. Aktivieren Sie im Block **Quarantäne und Backup** das Kontrollkästchen **Objekte löschen nach**, und legen Sie den Zeitraum fest, nach dem Quarantäneobjekte automatisch gelöscht werden sollen.

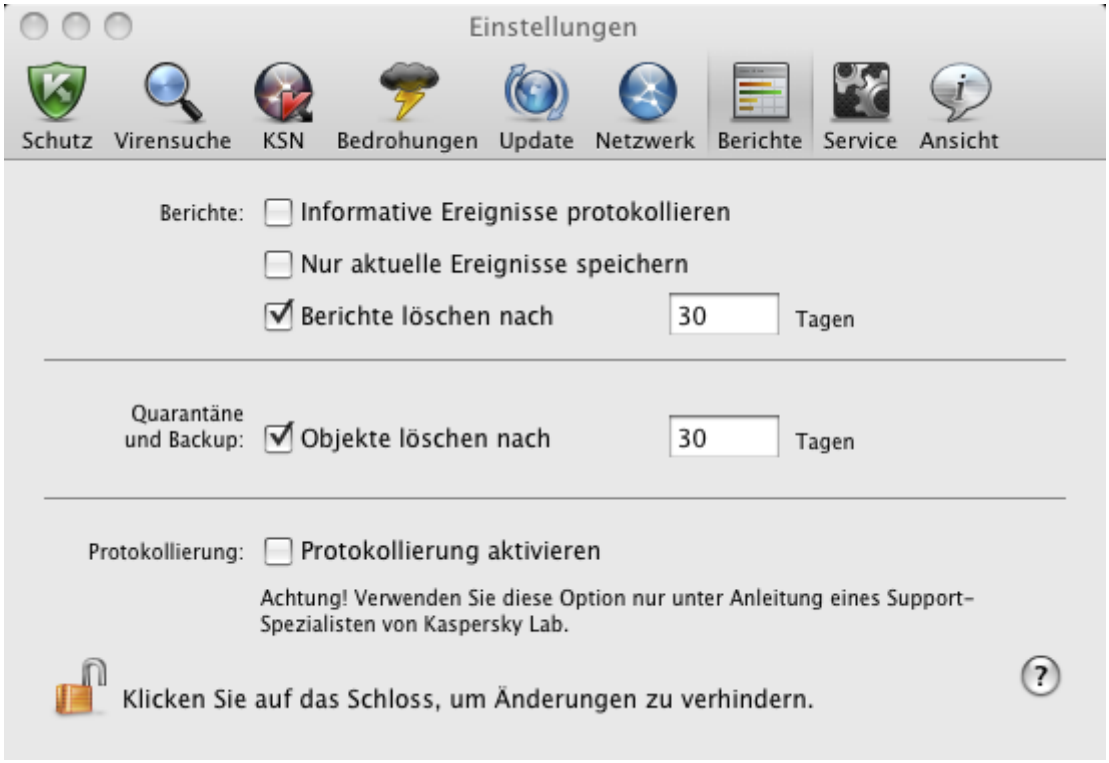

Abbildung 56. Programmkonfigurationsfenster. Berichte

TEILNAHME AM KASPERSKY SECURITY NETWORK

Jeden Tag taucht eine Vielzahl neuer Bedrohungen auf. Um ein schnelles Sammeln von Informationen über die Typen und Quellen neuer Bedrohungen zu gewährleisten und die Entwicklung entsprechender Neutralisierungsmethoden zu beschleunigen, können Sie sich dem Kaspersky Security Network anschließen.

Kaspersky Security Network (KSN) ist eine Infrastruktur der Online-Dienste und -Services, die den Zugriff auf die aktuelle Wissensdatenbank von Kaspersky Lab über den "Ruf" der Dateien, Internet-Ressourcen und Programme bietet. Durch die Verwendung der Daten des Kaspersky Security Network wird die Geschwindigkeit der Reaktion von Kaspersky Anti-Virus auf neue Bedrohungen und die Leistungsfähigkeit einiger Komponenten erhöht. Außerdem wird dadurch das Risiko verringert, dass Fehlalarme auftreten.

Bei Teilnahme am Kaspersky Security Network wird eine bestimmte Statistik, die während der Ausführung von Kaspersky Anti-Virus auf Ihrem Computer erstellt wird, automatisch an Kaspersky Lab übermittelt.

Es werden keine persönlichen Daten gesammelt, verarbeitet oder gespeichert.

Die Teilnahme am Kaspersky Security Network ist freiwillig. In der Regel entscheiden Sie im Verlauf der Installation von Kaspersky Anti-Virus über die Teilnahme. Allerdings können Sie Ihre Entscheidung jederzeit ändern.

Um Kaspersky Security Network zu aktivieren, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Programmkonfigurationsfenster (auf Seite 35), und wählen Sie die Registerkarte **KSN** aus (siehe Abbildung unten).

2. Klicken Sie im Block **Allgemein** auf die Schaltfläche **Vollständigen Text der Vereinbarung lesen**, um die Bestimmung über die Nutzung von Kaspersky Security Network anzuzeigen. Wenn Sie mit allen Punkten der Bestimmung einverstanden sind, aktivieren Sie das Kontrollkästchen **Ich bin mit den Teilnahmebedingungen an KSN einverstanden**.

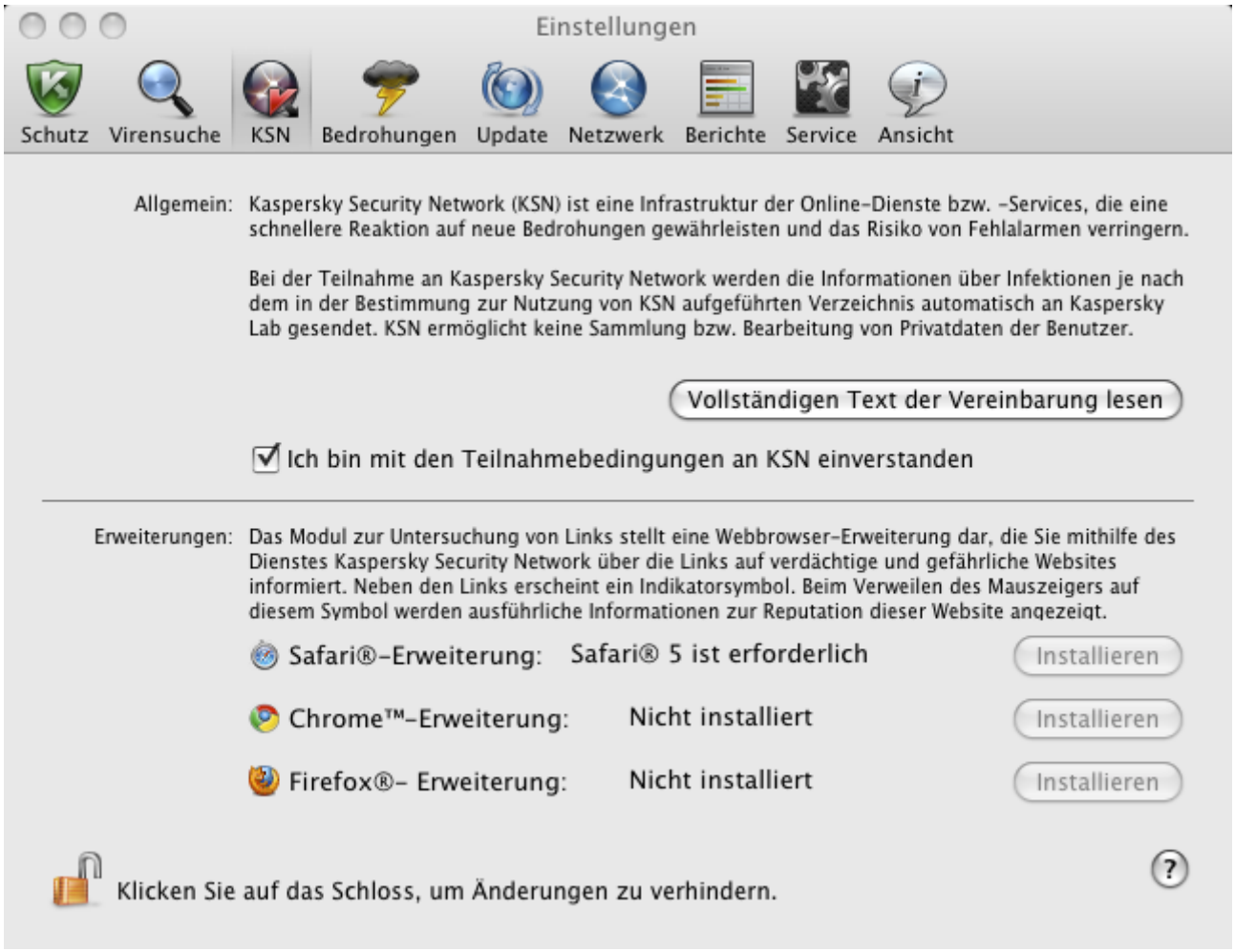
Einstellungen
Schutz
Virensuche
KSN
Bedrohungen
Update
Netzwerk
Berichte
Service
Ansicht
Allgemein:
Kaspersky Security Network (KSN) ist eine Infrastruktur der Online-Dienste bzw. -Services, die eine schnellere Reaktion auf neue Bedrohungen gewährleisten und das Risiko von Fehlalarmen verringern.
Bei der Teilnahme an Kaspersky Security Network werden die Informationen über Infektionen je nach dem in der Bestimmung zur Nutzung von KSN aufgeführten Verzeichnis automatisch an Kaspersky Lab gesendet. KSN ermöglicht keine Sammlung bzw. Bearbeitung von Privatdaten der Benutzer.
Vollständigen Text der Vereinbarung lesen
Ich bin mit den Teilnahmebedingungen an KSN einverstanden
Erweiterungen:
Das Modul zur Untersuchung von Links stellt eine Webbrowser-Erweiterung dar, die Sie mithilfe des Dienstes Kaspersky Security Network über die Links auf verdächtige und gefährliche Websites informiert. Neben den Links erscheint ein Indikatorsymbol. Beim Verweilen des Mauszeigers auf diesem Symbol werden ausführliche Informationen zur Reputation dieser Website angezeigt.
Safari®-Erweiterung: Safari® 5 ist erforderlich
Installieren
Chrome™-Erweiterung: Nicht installiert
Installieren
Firefox®- Erweiterung: Nicht installiert
Installieren
Klicken Sie auf das Schloss, um Änderungen zu verhindern.

Abbildung 57. Konfigurationsfenster. KSN

Durch die Teilnahme an Kaspersky Security Network können Sie die Erweiterungen für die meist verbreiteten Browser installieren: Safari®, Google™ Chrome™ и Firefox®. Durch die Verwendung der Daten von Kaspersky Security Network hebt Kaspersky Anti-Virus die Links im Browser je nach ihrer Gefährlichkeit hervor.

Um die Erweiterungen für Browser zu installieren, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Programmkonfigurationsfenster (auf Seite 35), und wählen Sie die Registerkarte **KSN** aus (siehe Abbildung oben).

2. Wählen Sie im Block **Erweiterungen** den Browser aus, für den Sie eine Erweiterung installieren wollen, und klicken auf **Installieren**.

BEDIENUNG DES PROGRAMMS ÜBER DIE BEFEHLSZEILE

Sie können Kaspersky Anti-Virus mit Hilfe der Befehlszeile steuern.

Syntax der Befehlszeile:

```
kav <Befehl> [Einstellungen]
```

Als <Befehl> können Sie verwenden:

- **help –** Hilfe zur Befehlssyntax, Anzeige einer Befehlsliste;
- **scan –** Untersuchung auf das Vorhandensein schädlicher Programme;
- **update –** Programm-Update starten;
- **rollback –** Rollback des letzten durchgeführten Update von Kaspersky Anti-Virus (für die Ausführung des Befehls braucht man Administratorrechte;
- **start** – Start einer Schutzkomponente oder einer Aufgabe;
- **stop –** Beenden der Arbeit einer Schutzkomponente oder Aufgabe (für die Ausführung des Befehls braucht man Administratorrechte);
- **status** – Aktuellen Status einer Komponente oder Aufgabe auf dem Bildschirm anzeigen;
- **statistics**– Die Statistik über die Arbeit einer Schutzkomponente oder einer Aufgabe auf dem Bildschirm anzeigen;
- **export –** Export der Arbeitseinstellungen einer Schutzkomponente oder Aufgabe;
- **import –** Import der Arbeitseinstellungen einer Schutzkomponente oder Aufgabe (für die Ausführung des Befehls braucht man Administratorrechte);
- **addkey –** Aktivierung des Programms mit Hilfe einer Schlüsseldatei (für die Ausführung des Befehls braucht man Administratorrechte);
- **exit –** Abschluss der Programmarbeit (für die Ausführung des Befehls braucht man Administratorrechte).

Jedem Befehl entspricht eine bestimmte Auswahl von Parametern.

IN DIESEM ABSCHNITT

Hilfe anzeigen 105

Virensuche 105

Programm-Update 107

Rollback zum vorherigen Update 108

Beenden einer Komponente oder einer Aufgabe 109

Statistik über die Arbeit einer Komponente oder Aufgabe 110

Schutzparameter exportieren 110

Schutzparameter importieren 110

Programm aktivieren 111

Programm beenden 111

Rückgabecodes der Befehlszeile 111

HILFE ANZEIGEN

Zur Anzeige der Hilfe über die Syntax der Befehlszeile dient folgender Befehl:

```
kav [ -? | help ]
```

Um Hilfe über die Syntax eines konkreten Befehls zu erhalten, können Sie einen der folgenden Befehle verwenden:

```
kav <Befehl> -?
kav help <Befehl>
```

VIRENSUCHE

Eine Befehlszeile für den Start der Untersuchung eines Bereichs auf Viren sieht im Allgemeinen folgendermaßen aus:

```
kav scan [<Untersuchungsobjekt>] [<Aktion>] [<Dateitypen>] [<Ausnahmen>]
[<Berichtsparameter>] [<zusätzliche Parameter>]
```

Für die Virensuche können Sie auch die im Programm erstellten Aufgaben verwenden, indem Sie die nötige aus der Befehlszeile starten (siehe Abschnitt "Starten / Beenden einer Komponente oder einer Aufgabe" auf Seite 109). Dabei wird die Aufgabe mit den Parametern ausgeführt, die über die Oberfläche von Kaspersky Anti-Virus festgelegt wurden.

Beschreibung der Parameter

<Untersuchungsobjekt> – Der Parameter gibt eine Liste der Objekte an, die auf das Vorhandensein von schädlichem Code untersucht werden sollen. Der Parameter kann mehrere Werte aus der folgenden Liste enthalten. Die Werte werden durch Leerzeichen getrennt:

<files> - liste mit den Pfaden der Dateien und / oder Ordner für die Untersuchung. Die Angabe des absoluten oder relativen Pfads der Datei ist zulässig. Als Trennzeichen für die Elemente der Liste dient das Leerzeichen. Kommentare:

- wenn der Objektname oder der Pfad eine Lücke oder spezielle Symbole enthält ($, &, @ usw.), muss er durch einfache Einführungszeichen eingeschlossen werden, oder das ausgeschlossene Symbol muss auf der linken Seite durch einen Backslash getrennt werden;
- wenn ein konkreter Ordner angegeben wird, werden alle darin enthaltenen Dateien und Ordner untersucht.

-all – Vollständige Untersuchung des Computers;

-remdrives – Alle Wechseldatenträger;

-fixdrives – Alle lokalen Laufwerke;

-netdrives – Alle Netzlaufwerke;

-quarantine – Objekte, die in die Quarantäne verschoben wurden;

-@:<filelist.lst> – Pfad der Datei mit einer Liste der Objekte und Ordner, die untersucht werden sollen. Die Datei muss das Textformat besitzen. Jedes Untersuchungsobjekt muss in einer separaten Zeile stehen. Nur die Angabe des absoluten Pfads der Datei ist zulässig.

Wenn keine Objekte für die Untersuchung angegeben wurden, führt Kaspersky Anti-Virus die Aufgabe zur **Virensuche** mit den Einstellungen aus, die in der Programmoberfläche festgelegt wurden.

<Aktion> – Der Parameter bestimmt die Aktionen mit einem schädlichen Objekt, das während der Untersuchung gefunden wird. Wenn der Parameter nicht angegeben wird, wird standardmäßig die Aktion ausgeführt, die dem Wert **-i8** entspricht. Folgende Varianten stehen zur Auswahl:

-i0- Keine Aktion ausführen, nur Informationen im Bericht protokollieren;

-i1 – Infizierte Objekte desinfizieren; wenn die Desinfektion nicht möglich ist – überspringen;

-i2 – die infizierten Objekte desinfizieren, wenn eine Desinfektion unmöglich ist – löschen; keine Container löschen, außer den Containern mit dem Ausführungstitel (sfx-Archive);

-i3 - infizierte Objekte desinfizieren; wenn die Desinfektion nicht möglich ist – löschen; Container-Objekte vollständig löschen, wenn die darin enthaltenen infizierten Dateien nicht gelöscht werden können;

-i4 - infizierte Objekte löschen; Container-Objekte vollständig löschen, wenn die darin enthaltenen infizierten Dateien nicht gelöscht werden können;

-i8 - beim Fund eines infizierten Objekts den Benutzer nach der Aktion fragen; Diese Aktion wird standardmäßig verwendet.

-i9 - den Benutzer nach der Aktion fragen, wenn die Untersuchung abgeschlossen wird.

<Dateitypen> – Der Parameter bestimmt die Typen der Dateien, die der Virenuntersuchung unterzogen werden. Wenn der Parameter nicht angegeben wird, werden standardmäßig nur infizierbare Dateien nach ihrem Inhalt untersucht. Folgende Varianten stehen zur Auswahl:

-fe – Nur infizierbare Dateien nach Erweiterung untersuchen;

-fi – Nur infizierbare Dateien nach Inhalt untersuchen (standardmäßig);

-fa – Alle Dateien untersuchen.

<Ausnahmen> – Der Parameter bestimmt die Objekte, die von der Untersuchung ausgeschlossen werden sollen. Man kann einige Parameter aus der folgenden Liste aufführen und diese in Probleme aufteilen:

-e:a – Archive nicht untersuchen;

-e:b – Mail-Datenbanken nicht untersuchen;

-e:m – E-Mail-Nachrichten im Textformat nicht untersuchen;

-e:<mask> – Objekte nicht nach einer Maske untersuchen (siehe Abschnitt "Zulässige Ausschlussmarken für Dateien" auf Seite 117);

-e:<seconds> – Objekte überspringen, deren Untersuchung länger dauert, als der durch den Parameter in Sekunden angegebene Zeitraum;

-es:<size> – Objekte überspringen, deren Größe den angegebenen Wert in Megabyte übersteigt.

<Berichtsparameter> – Der Parameter bestimmt das Format des Berichts über die Untersuchungsergebnisse. Die Verwendung eines absoluten oder relativen Pfads zur Datei für eine Berichtsspeicherung ist zulässig. Wenn der Parameter nicht angegeben wird, werden die Untersuchungsergebnisse auf dem Bildschirm angezeigt, alle Ereignisse werden angezeigt.

-r:<report_file> – Nur wichtige Ereignisse in der angegebenen Berichtsdatei protokollieren;

-ra:<report_file> – Alle Ereignisse in der angegebenen Berichtsdatei protokollieren.

<zusätzliche Einstellungen> – Einstellungen, die die Verwendung von Technologien zur Virenuntersuchung und der Konfigurationsdatei festlegen:

-iSwift=<on|off> – Verwendung der Technologie iSwift aktivieren / deaktivieren;

-c:<Name_der Konfigurationsdatei> – bestimmt den Pfad zur Konfigurationsdatei, die die Arbeitseinstellungen des Programms bei der Ausführung der Aufgaben zur Virensuche enthält. Die Angabe des absoluten oder relativen Pfads der Datei ist zulässig. Wenn kein Parameter festgelegt ist, werden neben den Werten, die bereits in der Befehlszeile angegeben sind, Werte benutzt, die auf der Programmoberfläche festgelegt sind.

Beispiel:

Eine Untersuchung der Ordner ~/Documents, /Applications und der Datei my test.exe starten:

```
kav scan ~/Documents /Applications 'my test.exe'
```

Untersuchung der Objekte, deren Liste in der Datei object2scan.txt angegeben ist. Für die Arbeit soll die Konfigurationsdatei scan_settings.txt verwendet werden. Über die Untersuchungsergebnisse soll ein Bericht erstellt werden, in dem alle Ereignisse aufgezeichnet werden:

```
kav scan -@:objects2scan.txt -c:scan_settings.txt -ra:scan.log
```

Beispiel für die Konfigurationsdatei:

```
-netdrives -@:objects2scan.txt -ra:scan.log
```

PROGRAMM-UPDATE

Der Befehl für das Update der Programm-Module und Antiviren-Datenbanken des Programms besitzt folgende Syntax:

```
avp.com UPDATE [<Updatequelle>] [/APP=<on|off>] [<Berichtsparameter>]
[<erweiterte_Einstellungen>]
```

Beschreibung der Parameter

<Updatequelle> – HTTP-, FTP-Server oder ein Netzwerk- oder Lokalordner zum Download von Updates. Wenn der Pfad nicht angegeben wird, wird die Updatequelle aus den Parametern des Diensts für das Programm-Update übernommen.

/APP=<on|off> – Update der Programm-Module aktivieren / deaktivieren.

<Berichtsparameter> – Der Parameter bestimmt das Format des Berichts über die Untersuchungsergebnisse. Die Angabe des absoluten oder relativen Pfads der Datei ist zulässig. Wenn der Parameter nicht angegeben wird, werden die Untersuchungsergebnisse auf dem Bildschirm angezeigt, alle Ereignisse werden angezeigt. Folgende Varianten stehen zur Auswahl:

-r:<report_file> – Nur wichtige Ereignisse in der angegebenen Berichtsdatei protokollieren;

/RA:<report_file> – Alle Ereignisse in der angegebenen Berichtsdatei protokollieren.

<zusätzliche Parameter> – Parameter, der die Verwendung von der Konfigurationsdatei festlegt.

/C: <Name_der_Konfigurationsdatei> – bestimmt den Pfad der Konfigurationsdatei, in der die Parameter für die Arbeit des Programms bei der Updateausführung enthalten sind. Die Angabe des absoluten oder relativen Pfads der Datei ist zulässig. Wenn der Parameter nicht angegeben wird, werden die Werte verwendet, die über die Programmoberfläche festgelegt wurden.

Beispiel:

Die Datenbanken des Programms aus der Quelle standardmäßig aktualisieren, alle Ereignisse im Bericht aufzeichnen:

```
kav update -ra:avbases_upd.txt
```

Update der Programm-Module von Kaspersky Anti-Virus, die Parameter der Konfigurationsdatei updateapp.ini verwenden:

```
kav update -app=on -c:updateapp.ini
```

ROLLBACK ZUM VORHERIGEN UPDATE

Befehlssyntax:

```
kav rollback [<Berichtsparameter>]
```

Für die Ausführung des Befehls braucht man Administratorrechte.

Beschreibung der Parameter

<Berichtsparameter> – Parameter, der das Format des Berichts über die Untersuchungsergebnisse bestimmt. Die Angabe des absoluten und relativen Pfads der Datei ist zulässig. Wenn der Parameter nicht angegeben wird, werden die Untersuchungsergebnisse auf dem Bildschirm angezeigt, alle Ereignisse werden angezeigt.

-r:<report_file> – Nur wichtige Ereignisse in der angegebenen Berichtsdatei protokollieren;

/RA:<report_file> – Alle Ereignisse in der angegebenen Berichtsdatei protokollieren. Die Angabe des absoluten oder relativen Pfads der Datei ist zulässig. Wenn der Parameter nicht angegeben wird, werden die Untersuchungsergebnisse auf dem Bildschirm angezeigt, alle Ereignisse werden angezeigt.

Beispiel:

```
kav rollback -ra:rollback.txt
```

BEENDEN EINER KOMPONENTE ODER EINER AUFGABE

Syntax des start-Befehls:

```
kav start <Profil|Aufgabenname> [<Berichtsparameter>]
```

Syntax des stop-Befehls:

```
kav stop <Profil|Aufgabenname>
```

Für die Ausführung des Befehls braucht man Administratorrechte.

Beschreibung der Parameter

<Berichtsparameter> – Der Parameter bestimmt das Format des Berichts über die Untersuchungsergebnisse. Die Angabe des absoluten und relativen Pfads der Datei ist zulässig. Wenn der Parameter nicht angegeben wird, werden die Untersuchungsergebnisse auf dem Bildschirm angezeigt, alle Ereignisse werden angezeigt. Folgende Varianten stehen zur Auswahl:

-r:<report_file> – Nur wichtige Ereignisse in der angegebenen Berichtsdatei protokollieren;

/RA:<report_file> – Alle Ereignisse in der angegebenen Berichtsdatei protokollieren. Die Angabe des absoluten oder relativen Pfads der Datei ist zulässig. Wenn der Parameter nicht angegeben wird, werden die Untersuchungsergebnisse auf dem Bildschirm angezeigt, alle Ereignisse werden angezeigt.

<Profil|Aufgabenname> – Einer der folgenden Werte wird angegeben:

file_monitoring (fm) – Datei-Anti-Virus;

scan_my_computer (full) – Aufgabe zur vollständigen Untersuchung des Computers;

scan_objects – Untersuchung von Objekten;

scan_quarantine – Quarantäne untersuchen;

scan_critical_areas (quick) - Aufgabe einer schneller Untersuchung des Computers;

updater – Updateaufgabe;

rollback – Aufgabe Rollback des Updates.

Als Wert dieses Parameters können Sie auch den Namen der vom Benutzer erstellten Aufgabe zur Virensuche angeben.

Die aus der Befehlszeile gestarteten Komponenten und Aufgaben werden mit den Parametern ausgeführt, die über die Programmoberfläche festgelegt wurden.

Beispiel:

Um Datei-Anti-Virus zu aktivieren, geben Sie in der Befehlszeile ein:

```
kav start fm
```

Um die Aufgabe zur vollständigen Untersuchung zu beenden, geben Sie in der Befehlszeile ein:

```
kav stop scan_my_computer
```

STATISTIK ÜBER DIE ARBEIT EINER KOMPONENTE ODER AUFGABE

Syntax des status-Befehls:

```
kav status [<Profil|Aufgabenname>]
```

Syntax des statistics-Befehls:

```
kav statistics <Profil|Aufgabenname>
```

Beschreibung der Parameter

<Profil|Taskname> – wird einer der für den Befehl start / stop aufgelisteten Werte angegeben. (siehe Abschnitt "Arbeit der Komponente oder Aufgabe starten / beenden" auf Seite 109)

Wenn der Befehl status ohne eine Wertangabe für den Parameter gestartet wird **<Profil|Aufgabenname>**, wird auf dem Bildschirm der aktuelle Status aller Aufgaben und Komponenten des Programms aufgezeigt. Für den Befehl statistics soll der Wert des Parameters **<Profil|Aufgabenname>** unbedingt angegeben werden.

SCHUTZPARAMETER EXPORTIEREN

Befehlssyntax:

```
kav export <Profil|Aufgabenname> <Dateiname>
```

Beschreibung der Parameter

<Profil|Aufgabenname> – wird einer der Werte angegeben, die für den Befehl aufgelistet sind start / stop (siehe Abschnitt "Arbeit der Komponente oder Aufgabe starten / beenden" auf Seite 109).

<Dateiname> – Pfad der Datei, in welche die Parameter vom Programm exportiert werden. Ein absoluter oder relativer Pfad kann angegeben werden.

Beispiel:

```
kav export fm fm_settings.txt – Textformat
```

SCHUTZPARAMETER IMPORTIEREN

Befehlssyntax:

```
kav import <Dateiname>
```

Für die Ausführung des Befehls braucht man Administratorrechte.

Beschreibung der Parameter

<Dateiname> – Pfad der Datei, in welche die Parameter vom Programm exportiert werden. Ein absoluter oder relativer Pfad kann angegeben werden.

Beispiel:

```
kav import settings.dat
```

PROGRAMM AKTIVIEREN

Die Aktivierung von Kaspersky Anti-Virus kann durch die Verwendung einer Schlüsseldatei ausgeführt werden.

Befehlssyntax:

```
kav addkey <Dateiname>
```

Für die Ausführung des Befehls braucht man Administratorrechte.

Beschreibung der Parameter

<Dateiname> – die Schlüsseldatei zum Programm mit der Erweiterung key.

Beispiel:

```
kav addkey 1AA111A1.key
```

PROGRAMM BEENDEN

Befehlssyntax:

```
kav exit
```

Für die Ausführung des Befehls braucht man Administratorrechte.

RÜCKGABECODES DER BEFEHLSZEILE

Die allgemeinen Codes können von einem beliebigen Befehl der Befehlszeile zurückgegeben werden. Zu den Rückgabecodes für Aufgaben zählen die allgemeinen Codes sowie spezifische Codes für einen konkreten Aufgabentyp.

Allgemeine Rückgabecodes:

- 0 – Operation wurde erfolgreich ausgeführt.
- 1 – Ungültiger Parameterwert.
- 2 – Unbekannter Fehler.
- 3 – Fehler bei Ausgabenausführung.

- 4 – Aufgabenausführung wurde abgebrochen.

Rückgabecodes für Aufgaben zur Virensuche:

- 101 – Alle gefährlichen Objekte wurden verarbeitet.
- 102 – Es wurden gefährliche Objekte gefunden.

KONTAKTAUFNAHME MIT DEM TECHNISCHEN SUPPORT

Wenn Sie Kaspersky Anti-Virus bereits erworben haben, können Sie von den Spezialisten des technischen Supports per Telefon oder über das Internet Informationen darüber erhalten. Die Support-Spezialisten beantworten Ihre Fragen, die die Installation und Verwendung des Programms betreffen und nicht in der Hilfe beschrieben werden. Wenn Ihr Computer infiziert wurde, helfen sie Ihnen auch dabei, die Folgen der Infizierung zu beheben.

➧ *Um Informationen über die Methoden des Support-Erhalts von Kaspersky Anti-Virus*

öffnen Sie das Programmhauptfenster (siehe Seite 34), und klicken Sie auf die Schaltfläche .

Lesen Sie sich vor der Kontaktaufnahme mit dem technischen Support die Supportregeln (http://support.kaspersky.com/de/support/rules) durch.

Wenn bei Ihnen während der Benutzung von Kaspersky Anti-Virus ein Problem auftritt, vergewissern Sie sich zuerst, ob seine Lösungsmethode in der Dokumentation, im Handbuch, im Knowledge Base auf der Webseite des Technischen Supports von Kaspersky Lab oder auf dem Benutzerforum beschrieben ist (siehe Abschnitt "Zusätzliche Informationsquellen" auf Seite 17). Wenn Sie keine Lösung für Ihr Problem finden können, empfehlen wir Ihnen, sich an den technischen Support von Kaspersky Lab zu wenden.

Beachten Sie in diesem Zusammenhang, dass Sie als Benutzer einer kommerziellen Version von Kaspersky Anti-Virus registriert sein müssen, um den technischen Support in Anspruch nehmen zu können. Die Benutzer von Testversionen der Anwendung besitzen keinen Anspruch auf technischen Support.

Wenn Kaspersky Anti-Virus mit Hilfe eines Aktivierungscodes aktiviert wird, wird die Registrierung des Benutzers vom Aktivierungsassistent durchgeführt (siehe Abschnitt "Aktivierung Kaspersky Anti-Virus" auf Seite 29).

Wenn Sie Kaspersky Anti-Virus mit Hilfe einer Schlüsseldatei aktivieren, gehen Sie unmittelbar durch den Registrierungsvorgang auf der Webseite des Technischen Supports (http://www.kaspersky.com/de/support).

Die Kundennummer und das Kennwort, die Sie bei der Registrierung erhalten, sind für den Zugriff auf das Portal "Mein Kaspersky" erforderlich. Dies ist der persönliche Bereich eines Benutzers auf der Webseite des technischen Supports. Im Portal "Mein Kaspersky" können Sie folgende Aktionen ausführen:

- eine Anfrage an den technischen Support schicken, ohne sich vorher anzumelden
- ohne Verwendung von E-Mails mit dem technischen Support korrespondieren
- den Status Ihrer Anfragen in Echtzeit verfolgen
- den vollständigen Verlauf Ihrer Anfragen an den technischen Support nachlesen
- eine Sicherungskopie Ihrer Schlüsseldatei abrufen.

E-Mail-Anfrage an den technischen Support

Um Kontakt mit dem technischen Support aufzunehmen, rufen Sie das Kontaktformular unter http://www.kaspersky.de/kontakt) auf. Rufen Sie auf der daraufhin automatisch angezeigten Webseite des technischen Supports Ihr Personal Cabinet auf, und füllen Sie das Anfrageformular aus.

Die Anfrage kann in Deutsch, Englisch, Französisch, Spanisch oder Russisch erfolgen.

Bei einer Anfrage per E-Mail ist die Angabe der **Kundennummer**, die Sie bei der Anmeldung über die Website des technischen Supports erhalten haben, und des **Kennworts** erforderlich.

Beschreiben Sie im Webformular das aufgetretene Problem möglichst genau. Geben Sie Folgendes in den obligatorischen Feldern an:

- **Typ der Anfrage**: Wählen Sie die Problemart aus, der Ihr Problem möglichst nahe kommt. Wenn Sie kein passendes Thema finden, wählen Sie "Allgemeine Frage" aus.
- **Name und Versionsnummer des Programms**:
- **Anfragetext**: Beschreiben Sie das Problem möglichst genau.
- **Kundennummer und Kennwort**: Geben Sie die Kundennummer und das Kennwort an, die Sie bei der Anmeldung auf der Support-Webseite erhalten haben.
- **E-Mail-Adresse**: An diese Adresse senden die Spezialisten des technischen Supports die Antwort auf Ihre Frage.

Die Mitarbeiter des technischen Supports senden die Antworten auf Ihre Fragen an die E-Mail-Adresse, die Sie in Ihrer Anfrage angegeben haben.

Telefonischer Technischer Support

Zur Lösung dringender Probleme können Sie jederzeit Ihren lokalen technischen Support anrufen. Wenn Sie sich an den russischsprachigen (http://support.kaspersky.ru/support/support_local) oder internationalen (http://support.kaspersky.com/de/support/international) technischen Support wenden, um Hilfe zu erhalten, vergessen Sie bitte nicht, die dafür erforderlichen Informationen (http://support.kaspersky.com/de/support/details) über Ihren Computer und das installierte Antiviren-Programm bereitzuhalten. Dadurch können Ihnen unsere Spezialisten schneller behilflich sein.

Protokolldatei erstellen

Während der Arbeit von Kaspersky Anti-Virus können Fehler auftreten, deren Ursache höchstwahrscheinlich in einem Konflikt von Kaspersky Anti-Virus mit der Software liegt, die auf Ihrem Computer installiert ist. Damit die Support-Spezialisten von Kaspersky Lab Sie bei der Lösung Ihres Problems unterstützen können, kann es sein, dass der Support Sie auffordert, eine Protokolldatei zu erstellen.

Gehen Sie folgendermaßen vor, um eine Protokolldatei zu erstellen:

1. Öffnen Sie das Programmkonfigurationsfenster, und wählen Sie die Registerkarte **Berichte**:
2. Aktivieren Sie im Block **Protokollierung** das Kontrollkästchen **Protokollierung aktivieren**.
3. Starten Sie Kaspersky Anti-Virus neu, um den Protokollierungsvorgang zu starten.

Verwenden Sie dieses Fenster nur unter Anleitung eines Support-Experten von Kaspersky Lab.

Protokolldateien können ein bedeutendes Volumen des Laufwerks einnehmen. Nach der Arbeit mit den Protokolldateien wird es empfohlen, ihre Erstellung zu deaktivieren. Deaktivieren Sie dazu das Kontrollkästchen **Protokollierung aktivieren** auf der Registerkarte **Berichte** des Programmkonfigurationsfensters. Starten Sie danach Kaspersky Anti-Virus neu.

ANHÄNGE

Hier erhalten Sie Hilfe zu den Formaten der zu untersuchenden Dateien und den zulässigen Ausschlussmasken, die bei der Konfiguration von Kaspersky Anti-Virus verwendet werden.

In diesem Abschnitt

Liste der Objekte, die auf ihre Erweiterung untersucht werden 115

Zulässige Ausschlussmasken für Dateien 117

Zulässige Ausschlussmasken gemäß der Klassifikation der Viren-Enzyklopädie 118

LISTE DER OBJEKTE, DIE AUF IHRE ERWEITERUNG UNTERSUCHT WERDEN

Wenn Sie bei der Konfiguration von Datei-Anti-Virus (siehe Abschnitt "Bestimmung von Typen der untersuchten Dateien" auf Seite 61) oder von den Aufgaben Antiviren-Suche (siehe Abschnitt "Bestimmung von Typen der untersuchten Dateien" auf Seite 76) die Variante **Programme und Dokumente (nach Erweiterung) untersuchen** ausgewählt haben, werden die Objekte mit den unten angegebenen Erweiterungen auf Viren untersucht:

com – Ausführbare Programmdatei für Microsoft Windows mit einer maximalen Größe von 64 KB;

exe – Ausführbare Datei, selbstextrahierendes Archiv für Microsoft Windows;

sys – Systemdatei für Microsoft Windows;

prg – Text des Programms dBase, Clipper oder Microsoft Visual FoxPro, Programm des Pakets WAVmaker;

bin – Binärdatei für Microsoft Windows;

bat – Datei einer Batchaufgabe für Microsoft Windows;

cmd – Befehlsdatei für Microsoft Windows NT (entspricht einer bat-Datei für DOS), OS/2;

dpl – Komprimierte Bibliothek für Borland Delphi;

dll – Dynamic Link Library für Microsoft Windows;

scr – Bildschirmschonerdatei für Microsoft Windows;

cpl – Systemsteuerungsmodul (control panel) für Microsoft Windows;

ocx – Microsoft OLE-Objekt (Object Linking and Embedding);

tsp – Programm für Microsoft Windows, das im Timesharingmodus arbeitet;

drv – Treiber für ein virtuelles Microsoft Windows-Gerät;

vxd – Treiber für ein virtuelles Microsoft Windows-Gerät;

pif – Datei für Microsoft Windows mit Informationen zu einem Programm;

lnk – Linkdatei für Microsoft Windows;

reg – Registrierungsschlüsseldatei für Microsoft Windows-Registrierung;

ini – Initialisierungsdatei für Microsoft Windows;

cla – Java-Klasse;

vbs – Visual Basic-Skript;

vbe – BIOS-Video-Erweiterung;

js, *jse* – JavaScript-Quelltext;

htm – Hypertext-Dokument;

htt – Hypertext-Dokumentvorlage für Microsoft Windows;

hta – Hypertext-Programm für Microsoft Internet Explorer;

asp – Active Server Pages-Skript;

chm – Kompilierte HTML-Datei;

pht – HTML-Datei mit eingebetteten PHP-Skripts;

php – Skript, das in eine HTML-Datei eingebettet wird;

wsh – Datei für Microsoft Windows Script Host;

wsf – Microsoft Windows-Skript;

the – Bildschirmschonerdatei für den Arbeitsplatz von Microsoft Windows 95;

hlp – Hilfedatei im Format Win Help;

eml – E-Mail für Microsoft Outlook Express;

nws – neue E-Mail für Microsoft Outlook Express;

msg – E-Mail für Microsoft Mail;

plg – E-Mail-Nachricht;

mbx – Endung für gespeicherte Nachricht in Microsoft Office Outlook;

*doc** – Dokumente für Microsoft Office Word, z.B: doc – Dokument für Microsoft Office Word, docx – Dokument für Microsoft Office Word 2007 mit XML-Unterstützung, docm – Dokument für Microsoft Office Word 2007 mit Makro-Unterstützung;

*dot** – Dokumentvorlage in Microsoft Office Word, z.B. dot – Dokumentvorlage in Microsoft Office Word, dotx – Dokumentvorlage in Microsoft Office Word 2007, dotm – Dokumentvorlage in Microsoft Office Word 2007 mit Makrounterstützung;

fpm – Datenbankprogramm, Startdatei für Microsoft Visual FoxPro;

rtf – Rich Text Format-Dokument;

shs – Datenauszug für Shell Scrap Object Handler;

dwg – AutoCAD-Dokument;

msi – Paket für Microsoft Windows Installer;

otm – VBA-Projekt für Microsoft Office Outlook;

pdf – Dokument für Adobe Acrobat;

swf – Objekt für Shockwave Flash;

jpg, *jpeg*, *png* – Komprimierte Bilddatei;

emf – Enhanced Metafile; Folgegeneration einer Metadatei des Betriebssystems Microsoft Windows;

ico – Symboldatei;

ov? – ausführbare Datei für MS DOS;

*xl** – Dokumente und Dateien für Microsoft Office Excel, z.B.: xla – Erweiterung für Microsoft Office Excel, xlc – Diagramm, xlt – Dokumentvorlage, xlsx – Arbeitsblatt für Microsoft Office Excel 2007, xltm – Arbeitsblatt für Microsoft Office Excel 2007 mit Makro-Unterstützung, xlsb – Arbeitsblatt für Microsoft Office Excel 2007 im Binärformat (nicht XML), xltx – Vorlage für Microsoft Office Excel 2007, xlsm – Vorlage für Microsoft Office Excel 2007 mit Makro-Unterstützung, xlam – Konfigurationsdatei für Microsoft Office Excel 2007 mit Makro-Unterstützung;

*pp** - Dokumente und Dateien für Microsoft Office PowerPoint, z.B.: pps – Folie für Microsoft Office PowerPoint, ppt – Präsentation, pptx – Präsentation für Microsoft Office PowerPoint 2007, pptm – Präsentation für Microsoft Office PowerPoint 2007 mit Makro-Unterstützung, potx – Präsentationsvorlage für Microsoft Office PowerPoint 2007, potm – Präsentationsvorlage für Microsoft Office PowerPoint 2007 mit Makro-Unterstützung, ppsx – Folienpräsentation für Microsoft Office PowerPoint 2007, ppsm – Folienpräsentation für Microsoft Office PowerPoint 2007 mit Makro-Unterstützung, ppam – Konfigurationsdatei für Microsoft Office PowerPoint 2007 mit Makro-Unterstützung;

*md** – Dokumente und Dateien für Microsoft Office Access, z.B: mda – Arbeitsgruppe für Microsoft Office Access, mdb – Datenbank usw.;

sldx – Dia in Microsoft Office PowerPoint 2007;

sldm – Dia in Microsoft Office PowerPoint 2007 mit Makrounterstützung;

thmx – Thema für Microsoft Office 2007.

Das tatsächliche Format einer Datei kann von dem Format, das in der Dateierweiterung angegeben ist, abweichen.

ZULÄSSIGE AUSSCHLUSSMASKEN FÜR DATEIEN

Hier werden Beispiele für zulässige Masken genannt, die Sie beim Erstellen der Liste auszuschließender Dateien verwenden können:

1. Masken ohne Dateipfad:
   - ***.zip** — Alle Dateien mit der Endung zip;
   - ***.zi?** – Alle Dateien mit der Endung zi?, wobei anstelle von ? ein beliebiges Zeichen stehen kann;
   - **test** – Alle Dateien mit dem Namen test.
2. Masken mit absolutem Dateipfad:
   - **/dir/*** oder **/dir/** – Alle Dateien im Ordner /dir/;
   - **/dir/*.zip** – Alle Dateien mit der Endung zip im Ordner /dir/;

- **/dir/*.zi?** – Alle Dateien mit der Endung zi? im Ordner /dir/, wobei anstelle von ? ein beliebiges Zeichen stehen kann;
- **/dir/test** – alle Dateien mit dem Namen test im Ordner /dir/ und in allen darin eingelegten Ordnern.

3. Masken mit relativem Dateipfad:
   - **dir/*** oder **dir/** – Alle Dateien in Ordnern mit der Bezeichnung dir/;
   - **dir/*.zip** – Alle Dateien mit der Endung zip in Ordnern mit der Bezeichnung dir/;
   - **dir/*.zi?** – Alle Dateien mit der Endung zi? in Ordnern mit der Bezeichnung dir/, wobei anstelle von ? ein beliebiges Zeichen stehen kann;
   - **dir/test** – alle Dateien mit dem Namen test im Ordner /dir/ und in allen darin eingelegten Ordnern.

Die Verwendung der Ausnahmemaske * ist nur zulässig, wenn der Typ der auszuschließenden Bedrohung gemäß der Viren-Enzyklopädie angegeben wird. In diesem Fall wird die Bedrohung nicht in allen Objekten gefunden werden. Wenn diese Maske ohne Angabe eines Bedrohungstyps verwendet wird, entspricht dies dem Deaktivieren des Schutzes.

ZULÄSSIGE AUSSCHLUSSMASKEN GEMÄß DER KLASSIFIKATION DER VIREN-ENZYKLOPÄDIE

Wenn als Ausnahme eine Bedrohung mit einem bestimmten Status nach der Klassifikation der Viren-Enzyklopädie hinzugefügt wird, können Sie Folgendes angeben:

- Den vollständigen Namen der Bedrohung, wie er in der Viren-Enzyklopädie auf der Seite www.securelist.com/de/de/ genannt wird (http://www.securelist.com/de/) (beispielsweise, **not-a-virus:RiskWare.RemoteAdmin.RA.311** oder **Flooder.Win32.Fuxx**).
- Den Namen einer Bedrohung als Maske, z.B.:
  - **not-a-virus*** – Legale, aber potentiell gefährliche Programme sowie Scherzprogramme von der Untersuchung ausschließen.
  - ***Riskware.*** – Alle potentiell gefährlichen Programme des Typs Riskware von der Untersuchung ausschließen.
  - ***RemoteAdmin.*** – Alle Versionen von Programmen zur Fernverwaltung von der Untersuchung ausschließen.

Beispiele der Bedrohungsnamen können im Berichtsfenster auf der Registerkarte **Erfasst**, in der Quarantäne und im Backup, sowie in Pop-up-Meldungen (siehe Abschnitt "Meldungsfenster und Pop-up-Meldungen" auf Seite 36) über die Erfassung von gefährlichen Objekten eingesehen werden.

GLOSSAR

A

Aktive Lizenz

Lizenz, die momentan für die Arbeit des Kaspersky-Lab-Programms verwendet wird. Die Lizenz legt die Gültigkeitsdauer für den vollen Funktionsumfang sowie die Lizenzpolitik für das Programm fest. Im Programm kann nur ein Schlüssel den Status "aktiv" besitzen.

Archiv

Datei, die ein oder mehrere Objekte "enthält", die ihrerseits auch Archive sein können.

Ausnahme

Eine Ausnahme ist ein Objekt, das von der Untersuchung durch das Kaspersky-Lab-Programm ausgeschlossen wird. Von der Untersuchung können Dateien eines bestimmten Formats, Dateien nach Maske, bestimmte Bereiche (beispielsweise ein Ordner oder Programm) sowie Programmprozesse oder Objekte nach einem Bedrohungstyp gemäß der Klassifikation der Viren-Enzyklopädie ausgeschlossen werden. Für jede Aufgabe können individuelle Ausnahmen festgelegt werden.

B

Backup

Spezieller Speicher für Sicherungskopien von Objekten, die vor einer Desinfektion oder vor dem Löschen angelegt werden.

D

Dateimaske

Platzhalter für den Namen und die Erweiterung einer Datei, der aus allgemeinen Zeichen besteht. Die zwei wichtigsten Zeichen, die in Dateimasken verwendet werden sind * und ? (wobei * für eine beliebige Anzahl von beliebigen Zeichen und ? für ein beliebiges Einzelzeichen steht). Mit Hilfe dieser Zeichen kann jede beliebige Datei dargestellt werden. Beachten Sie, dass Name und Endung einer Datei stets durch einen Punkt getrennt werden.

Datenbank-Update

Eine Funktion, die vom Kaspersky-Lab-Programm ausgeführt wird und die es erlaubt, den aktuellen Zustand des Schutzes aufrecht zu erhalten. Dabei werden die Datenbanken von den Kaspersky-Lab-Updateservern auf den Computer kopiert und automatisch von der Anwendung übernommen.

Datenbanken

Datenbanken, die von den Kaspersky-Lab-Spezialisten gepflegt werden und eine genaue Beschreibung aller momentan existierenden Bedrohungen der Computersicherheit sowie Methoden zu ihrer Identifikation und Desinfektion enthalten. Die Datenbanken werden von Kaspersky Lab laufend aktualisiert, wenn neue Bedrohungen auftauchen.

Desinfektion von Objekten

Methode zur Bearbeitung von infizierten Objekten, bei der die Daten vollständig oder teilweise wiederhergestellt werden oder eine Entscheidung darüber getroffen wird, dass die Desinfektion von Objekten nicht möglich ist. Die Desinfektion von Objekten erfolgt auf Basis der Einträge in den Datenbänken. Bei der Desinfektion können Daten teilweise verloren gehen.

E

EMPFOHLENE STUFE

Sicherheitsstufe, deren Funktionsparameter von Kaspersky Lab empfohlen werden und die einen optimalen Schutz Ihres Computers gewährleistet. Diese Stufe wird in der Grundeinstellung verwendet.

F

FEHLALARM

Situation, in der ein virenfreies Objekt von der Kaspersky-Lab-Anwendung als infiziert eingestuft wird, weil sein Code Ähnlichkeit mit einem Virus aufweist.

G

GEFÄHRLICHES OBJEKT

Objekt, in dem sich ein Virus befindet. Es wird davor gewarnt, mit solchen Objekten zu arbeiten, weil dies zur Infektion des Computers führen kann. Beim Fund eines infizierten Objekts wird empfohlen, das Objekt mit Hilfe des Kaspersky-Lab-Programms zu desinfizieren oder, falls die Desinfektion nicht möglich ist, es zu löschen.

H

HEURISTISCHE ANALYSE

Erkennungstechnologie für Bedrohungen, die nicht mit Hilfe der Programmdatenbanken des Kaspersky Lab bestimmt werden können. Es wird erlaubt, Objekte zu finden, die verdächtig sind, durch einen unbekannten Virus oder eine neue Modifikation eines bekannten Virus infizierte zu sein.

Mit Hilfe der heuristischen Analyse werden bis zu 92 % der neuen Bedrohungen erkannt. Dieser Mechanismus ist sehr effektiv und führt nur selten zu einem Fehlalarm.

Dateien, die mit Hilfe der heuristischen Analyse gefunden werden, nennt man verdächtig.

I

INFIZIERTES OBJEKT

Objekt, das schädlichen Code enthält: Bei der Untersuchung des Objekts wurde erkannt, dass ein Abschnitt des Objektcodes vollständig mit dem Code einer bekannten Bedrohung übereinstimmt. Die Kaspersky-Lab-Spezialisten warnen davor, mit solchen Objekten zu arbeiten, weil dies zur Infektion Ihres Computers führen kann.

K

KASPERSKY-LAB-UPDATESERVER

Liste der HTTP- und FTP-Server von Kaspersky Lab, von denen das Programm die Updates für Datenbanken und Module auf Ihren Computer herunterlädt.

M

MAXIMALER SCHUTZ

Sicherheitsstufe, die Ihrem Computer den maximalen Schutz bietet, den die Anwendung gewährleisten kann. Auf dieser Sicherheitsstufe werden alle Dateien des Computers sowie Wechseldatenträger und Netzlaufwerke auf Viren untersucht.

MÖGLICHERWEISE INFIZIERTES OBJEKT

Objekt, dessen Code entweder den modifizierten Code eines bekannten Virus oder einen Code, der einem Virus gleicht, enthält, der Kaspersky Lab aber bisher nicht bekannt ist. Infizierte Dateien können mit Hilfe der heuristischen Analyse gefunden werden.

O

OBJEKT BLOCKIEREN

Der Zugriff externer Programme auf ein Objekt wird verboten. Ein blockiertes Objekt kann nicht gelesen, ausgeführt oder geändert werden.

OLE-OBJEKT

Objekt, das an eine andere Datei angehängt oder darin eingebettet ist. Das Kaspersky-Lab-Programm erlaubt es, OLE-Objekte auf das Vorhandensein von Viren zu untersuchen. Wenn Sie beispielsweise eine beliebige Tabelle aus Microsoft Office Excel in ein Dokument des Typs Microsoft Office Word einfügen, wird die Tabelle als OLE-Objekt untersucht.

P

POTENTIELL INFIZIERBARES OBJEKT

Ein Objekt das aufgrund seiner Struktur seines Formats von einem Angreifer als "Container" benutzt werden kann, um ein schädliches Objekt zu platzieren oder weiterzuverbreiten. In der Regel sind dies ausführbare Dateien mit Erweiterungen wie com, exe, dll usw. Das Risiko des Eindringens und der Aktivierung von schädlichem Code ist für solche Dateien relativ hoch.

PROGRAMM AKTIVIEREN

Wechsel des Programms in einen voll funktionellen Modus. Zur Aktivierung des Programms braucht der Benutzer eine Lizenz.

Q

QUARANTÄNE

Ein bestimmter Ordner, in den alle möglicherweise infizierten Objekte verschoben werden, die bei der Untersuchung oder im Rahmen des Echtzeitschutzes gefunden werden.

R

RESERVELIZENZ

Lizenz, die für die Arbeit der Kaspersky-Lab-Anwendung hinzugefügt, aber nicht aktiviert wurde. Eine Reservelizenz wird aktiviert, wenn die Gültigkeit der aktiven Lizenz abläuft.

S

SCHUTZ

Funktionsmodus des Programms, in dem Objekte im Echtzeitmodus auf schädlichen Code untersucht werden.

Das Programm fängt jeden Versuch zum Öffnen, Schreiben und Ausführen eines Objekts ab, und durchsucht das Objekt nach Bedrohungen. Virenfreie Objekte werden für den Zugriff freigegeben, infizierte oder verdächtige Objekte werden gemäß den Aufgabenparametern verarbeitet (desinfiziert, gelöscht, in die Quarantäne verschoben).

SCHUTZSTATUS

Aktueller Schutzstatus, der das Sicherheitsniveau des Computers charakterisiert.

T

TECHNOLOGIE GROWL

Universelles Warnsystem im Betriebssystem Mac OS X. Unterstützt die installierten Arten von Meldungen: Außer den Pop-up-Meldungen besteht die Möglichkeit zu Audio-Meldungen, SMS- oder E-Mail-Meldungen.

Die äußere Form von Meldungen die mit Hilfe von Growl angezeigt werden, kann im Abschnitt Andere des Bereichs Systemkonfigurationen angepasst werden, wo Growl automatisch nach dem Download eingesetzt wird.

U

UNBEKANNTER VIRUS

Neuer Virus, über den noch keine Informationen in den Datenbanken vorhanden sind. Unbekannte Viren werden mit der heuristischen Analyse erkannt und erhalten den Status möglicherweise infiziert.

UPDATE

Vorgang, bei dem vorhandene Dateien (Datenbanken oder Programm-Module) durch neue Dateien ersetzt bzw. neue Dateien hinzugefügt werden. Die neuen Dateien werden von den Kaspersky-Lab-Updateservern heruntergeladen.

UPDATEPAKET

Dateipaket, das der Softwareaktualisierung dient, aus dem Internet kopiert und auf Ihrem Computer installiert wird.

V

VERDÄCHTIGES OBJEKT

Objekt, dessen Code entweder den modifizierten Code eines bekannten Virus oder einen Code, der einem Virus gleicht, enthält, der Kaspersky Lab aber bisher nicht bekannt ist. Verdächtige Objekte werden unter Einsatz der heuristischen Analyse erkannt.

W

WIEDERHERSTELLUNG

Ein Originalobjekt wird aus der Quarantäne oder aus dem Backup entweder an den ursprünglichen Ort, an dem das Objekt gespeichert war, bevor es in die Quarantäne verschoben, desinfiziert oder gelöscht wurde, oder in einen benutzerdefinierten Ordner verschoben.

KASPERSKY LAB

Kaspersky Lab ist ein weltweit bekannter Hersteller von Systemen, die Computer vor Viren und anderer Malware, Spam, Netzwerk- und Hackerangriffen schützen.

Seit 2008 gehört Kaspersky Lab international zu den vier führenden Unternehmen im Bereich der IT-Sicherheit für Endbenutzer (Rating des "IDC Worldwide Endpoint Security Revenue by Vendor"). Nach einer Studie des Marktforschungsinstituts COMCON TGI-Russia war Kaspersky Lab 2009 in Russland der beliebteste Hersteller von Schutzsystemen für Heimanwender.

Kaspersky Lab wurde 1997 in Russland gegründet. Inzwischen ist Kaspersky Lab ein international tätiger Konzern mit Hauptsitz in Moskau und verfügt über fünf regionale Niederlassungen, die in Russland, West- und Osteuropa, im Nahen Osten, in Afrika, Nord- und Südamerika, Japan, China und anderen Ländern aktiv sind. Das Unternehmen beschäftigt über 2.000 hochspezialisierte Mitarbeiter.

Produkte. Die Produkte von Kaspersky Lab schützen sowohl Heimanwender als auch Firmennetzwerke.

Die Palette der Heimanwender-Produkte umfasst Antiviren-Anwendungen für Desktops, Laptops, Smartphones und andere mobile Geräte.

Das Unternehmen bietet Programme und Services für den Schutz von Workstations, Datei- und Webservern, Mail-Gateways und Firewalls. In Verbindung mit Administrationstools ermöglichen es diese Lösungen, netzwerkweit einen effektiven automatisierten Schutz vor Computerbedrohungen aufzubauen. Die Produkte von Kaspersky Lab sind durch namhafte Testlabore zertifiziert, mit den Programmen der meisten Softwarehersteller kompatibel und für die Arbeit mit unterschiedlichen Hardwareplattformen optimiert.

Die Virenanalysten von Kaspersky Lab sind rund um die Uhr im Einsatz. Sie finden und analysieren jeden Tag Hunderte neuer Computerbedrohungen. Mit diesem Wissen entwickeln sie Mittel, um Gefahren zu erkennen und zu desinfizieren. Diese Informationen fließen in die Datenbanken ein, auf die die Kaspersky-Programme zurückgreifen. *Die Antiviren-Datenbanken von Kaspersky Lab werden stündlich aktualisiert*, *die Anti-Spam-Datenbanken im 5-Minuten-Takt*.

Technologien. Viele Technologien, die für ein modernes Antiviren-Programm unerlässlich sind, wurden ursprünglich von Kaspersky Lab entwickelt. Es spricht für sich, dass viele Softwarehersteller den Kernel von Kaspersky Anti-Virus in ihren Produkten einsetzen. Zu ihnen zählen SafeNet (USA), Alt-N Technologies (USA), Blue Coat Systems (USA), Check Point Software Technologies (Israel), Clearswift (UK), CommuniGate Systems (USA), Critical Path (Ireland), D-Link (Taiwan), M86 Security (USA), GFI (Malta), IBM (USA), Juniper Networks (USA), LANDesk (USA), Microsoft (USA), NETASQ (France), NETGEAR (USA), Parallels (Russia), SonicWALL (USA), WatchGuard Technologies (USA), ZyXEL Communications (Taiwan). Eine Vielzahl von innovativen Technologien des Unternehmens ist durch Patente geschützt.

Auszeichnungen. Im Verlauf eines kontinuierlichen Kampfes mit Computerbedrohungen hat Kaspersky Lab Hunderte von Auszeichnungen erworben. So wurde Kaspersky Anti-Virus 2010 in einem Test des anerkannten österreichischen Antiviren-Labors AV-Comparatives mit mehreren Premium-Awards Advanced+ ausgezeichnet. Die höchste Auszeichnung stellt für Kaspersky Lab aber das Vertrauen seiner Benutzer auf der ganzen Welt dar. Die Produkte und Technologien des Unternehmens schützen mehr als 300 Millionen Anwender. Über 200.000 Firmen zählen zu den Kunden von Kaspersky Lab.

Webseite von Kaspersky Lab:	http://www.kaspersky.com/de/
Viren-Enzyklopädie:	http://www.securelist.com/de/
Antiviren-Labor:	newvirus@kaspersky.com (nur zum Einsenden verdächtiger Objekte, die zuvor archiviert wurden) http://support.kaspersky.ru/virlab/helpdesk.html?LANG=de (für Fragen an die Virenanalytiker)
Webforum von Kaspersky Lab:	www.kaspersky.de/forum

INFORMATIONEN ZUM FREMDCODE

Zur Erstellung des Programms wird ein Code von fremden Herstellern verwendet.

IN DIESEM ABSCHNITT

Programmcode 124

Erarbeitungsmittel 130

Andere Informationen 134

PROGRAMMCODE

Bei der Entwicklung des Programms wurde der Programmcode von Drittherstellern verwendet.

IN DIESEM ABSCHNITT

ADOBE ABI-SAFE CONTAINERS 1.0 125

BOOST 1.39.0 125

CURL 7.19.3 125

EXPAT 1.2 125

FMT.H 126

GROWL 1.1.5 126

INFO-ZIP 5.51 127

LIBPNG 1.2.8 127

LIBUTF 127

LZMALIB 4.43 128

MD5.H 128

MD5.H 128

RFC1321-BASED (RSA-FREE) MD5 LIBRARY 128

SHA1.C 1.2 128

STLPORT 5.2.1 129

TINYXML 2.5.3 129

WEB-SOCKET-JS 129

ZLIB 1.0.8, 1.2.3 130

ADOBE ABI-SAFE CONTAINERS 1.0

Copyright (C) 2005, Adobe Systems Incorporated

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVEN SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

BOOST 1.39.0

Copyright (C) 2008, Beman Dawes

CURL 7.19.3

Copyright (C) 1996 - 2009, Daniel Stenberg (daniel@haxx.se)

COPYRIGHT AND PERMISSION NOTICE

Copyright (c) 1996 - 2009, Daniel Stenberg, <daniel@haxx.se>.

All rights reserved.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

EXPAT 1.2

Copyright (C) 1998 - 2000, Thai Open Source Software Center Ltd

---

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,

EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF

MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT.

IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

FMT.H

Copyright (C) 2002, Lucent Technologies

Permission to use, copy, modify, and distribute this software for any purpose without fee is hereby granted, provided that this entire notice is included in all copies of any software which is or includes a copy or modification of this software and in all copies of the supporting documentation for such software.

THIS SOFTWARE IS BEING PROVIDED "AS IS", WITHOUT ANY EXPRESS OR IMPLIED WARRANTY. IN PARTICULAR, NEITHER THE AUTHORS NOR LUCENT TECHNOLOGIES MAKE ANY REPRESENTATION OR WARRANTY OF ANY KIND CONCERNING THE MERCHANTABILITY OF THIS SOFTWARE OR ITS FITNESS FOR ANY PARTICULAR PURPOSE.

GROWL 1.1.5

Copyright (C) 2004, The Growl Project

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name of Growl nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)

HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

INFO-ZIP 5.51

Copyright (C) 1990-2007, Info-ZIP

For the purposes of this copyright and license, "Info-ZIP" is defined as the following set of individuals:

Mark Adler, John Bush, Karl Davis, Harald Denker, Jean-Michel Dubois, Jean-loup Gailly, Hunter Goatley, Ed Gordon, Ian Gorman, Chris Herborth, Dirk Haase, Greg Hartwig, Robert Heath, Jonathan Hudson, Paul Kienitz, David Kirschbaum, Johnny Lee, Onno van der Linden, Igor Mandrichenko, Steve P. Miller, Sergio Monesi, Keith Owens, George Petrov, Greg Roelofs, Kai Uwe Rommel, Steve Salisbury, Dave Smith, Steven M. Schweda, Christian Spieler, Cosmin Truta, Antoine Verheijen, Paul von Behren, Rich Wales, Mike White.

This software is provided "as is", without warranty of any kind, express or implied. In no event shall Info-ZIP or its contributors be held liable for any direct, indirect, incidental, special or consequential damages arising out of the use of or inability to use this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the above disclaimer and the following restrictions:

1. Redistributions of source code (in whole or in part) must retain the above copyright notice, definition, disclaimer, and this list of conditions.

2. Redistributions in binary form (compiled executables and libraries) must reproduce the above copyright notice, definition, disclaimer, and this list of conditions in documentation and/or other materials provided with the distribution. The sole exception to this condition is redistribution of a standard UnZipSFX binary (including SFXWiz) as part of a self-extracting archive; that is permitted without inclusion of this license, as long as the normal SFX banner has not been removed from the binary or disabled.

3. Altered versions--including, but not limited to, ports to new operating systems, existing ports with new graphical interfaces, versions with modified or added functionality, and dynamic, shared, or static library versions not from Info-ZIP--must be plainly marked as such and must not be misrepresented as being the original source or, if binaries, compiled from the original source. Such altered versions also must not be misrepresented as being Info-ZIP releases--including, but not limited to, labeling of the altered versions with the names "Info-ZIP" (or any variation thereof, including, but not limited to, different capitalizations), "Pocket UnZip," "WiZ" or "MacZip" without the explicit permission of Info-ZIP. Such altered versions are further prohibited from misrepresentative use of the Zip-Bugs or Info-ZIP e-mail addresses or the Info-ZIP URL(s), such as to imply Info-ZIP will provide support for the altered versions.

4. Info-ZIP retains the right to use the names "Info-ZIP," "Zip," "UnZip," "UnZipSFX," "WiZ," "Pocket UnZip," "Pocket Zip," and "MacZip" for its own source and binary releases.

LIBPNG 1.2.8

Copyright (C) 2004, 2006-2009, Glenn Randers-Pehrson

LIBUTF

Copyright (C) 2002, Lucent Technologies

Permission to use, copy, modify, and distribute this software for any purpose without fee is hereby granted, provided that this entire notice is included in all copies of any software which is or includes a copy or modification of this software and in all copies of the supporting documentation for such software.

THIS SOFTWARE IS BEING PROVIDED "AS IS", WITHOUT ANY EXPRESS OR IMPLIED WARRANTY. IN PARTICULAR, NEITHER THE AUTHORS NOR LUCENT ECHNOLOGIES MAKE ANY REPRESENTATION OR WARRANTY OF ANY KIND CONCERNING THE MERCHANTABILITY OF THIS SOFTWARE OR ITS FITNESS FOR ANY PARTICULAR PURPOSE.

LZMALIB 4.43

MD5.H

Copyright (C) 1999, Aladdin Enterprises

MD5.H

Copyright (C) 1990, RSA Data Security, Inc

License to copy and use this software is granted provided that it is identified as the "RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing this software or this function.

License is also granted to make and use derivative works provided that such works are identified as "derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing the derived work.

RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided "as is" without express or implied warranty of any kind.

These notices must be retained in any copies of any part of this documentation and/or software.

RFC1321-BASED (RSA-FREE) MD5 LIBRARY

Copyright (C) 1999, 2002, Aladdin Enterprises

SHA1.C 1.2

STLPORT 5.2.1

Copyright (C) 1994, Hewlett-Packard Company

Copyright (C) 1996-1999, Silicon Graphics Computer Systems, Inc.

Copyright (C) 1997, Moscow Center for SPARC Technology

Copyright (C) 1999-2003, Boris Fomitchev

This material is provided "as is", with absolutely no warranty expressed or implied. Any use is at your own risk.

Permission to use or copy this software for any purpose is hereby granted without fee, provided the above notices are retained on all copies. Permission to modify the code and to distribute modified code is granted, provided the above notices are retained, and a notice that the code was modified is included with the above copyright notice.

TINYXML 2.5.3

Copyright (C) 2000-2006, Lee Thomason

WEB-SOCKET-JS

Copyright (C) Hiroshi Ichikawa <http://gimite.net/en/>

Copyright (C) 2006, Adobe Systems Incorporated

Copyright (C) Hiroshi Ichikawa <http://gimite.net/en/>

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

- Neither the name of the <ORGANIZATION> nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright (C) 2006, Adobe Systems Incorporated

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

ZLIB 1.0.8, 1.2.3

Copyright (C) 1995-2010, Jean-loup Gailly and Mark Adler

ERARBEITUNGSMITTEL

Bei der Entwicklung des Programms wurden die Entwicklungstools und und andere Mittel von Drittherstellern verwendet.

IN DIESEM ABSCHNITT

GCC 4.0.1 130

GCC 4.0.1

Copyright (C) 1987, 1989, 1992, 1993, 1994, 1995, 1996, 1997, 1998, 1999, 2000, 2001, 2002, 2003, 2004, 2005 Free Software Foundation, Inc

---

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

one line to give the program's name and an idea of what it does.

Copyright (C) yyyy name of author

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author

Gnomovision comes with ABSOLUTELY NO WARRANTY; for details

type `show w'. This is free software, and you are welcome

to redistribute it under certain conditions; type `show c'

for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program `Gnomovision'

(which makes passes at compilers) written

by James Hacker.

signature of Ty Coon, 1 April 1989

Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License instead of this License.

ANDERE INFORMATIONEN

Zusätzliche Informationen zum Fremdcode.

Zur Überprüfung der elektronischen digitalen Signatur wird die Programmbibliothek für den Informationsschutz (PBSI) "Agava-C" eingesetzt, die von R-Alpha OOO entwickelt wurde.

Dieses Produkt enthält Programme oder kann Programme enthalten, die nach der freien GNU-Lizenz oder anderen vergleichbaren Open Source-Lizenzen an den Benutzer lizenziert (oder sublizenziert) werden, die dem Benutzer neben sonstigen Rechten gestatten, bestimmte Programme oder deren Teile zu kopieren, zu modifizieren und zu verteilen sowie auf den Quellcode zuzugreifen ("Open Source Software"). Sofern diese Lizenzen erfordern, dass der Quellcode für eine in einem ausführbaren, binären Format weitergegebene Software dem Nutzer ebenfalls zugänglich gemacht wird, wird der Quellcode nach einer entsprechenden Anforderung an source@kaspersky.com zur Verfügung gestellt bzw. mit der Software geliefert.

SACHREGISTER

A

Aktionen mit Objekten 65, 77, 94, 97
Aktivierungsassistent 29, 30, 31
Aktivierungscode 29, 30
Archive 61, 76

B

Backup 96
Bedrohungstypen 52
Benachrichtigungen 36
Benutzerdefinierte Installation 23
Berichte 98, 100

D

Datei-Anti-Virus
- Aktivierung / Deaktivierung 57, 59
- Heuristische Analyse 64
- Schutzbereich 62
- Sicherheitsstufe 60
- Statistik über die Arbeit der Komponente 66
- Untersuchung optimieren 61
- Untersuchung von zusammengesetzten Dateien 61
- Untersuchungstechnologie 64
- Wiederherstellung der Standardeinstellungen 66

Datenbanken 83, 85, 87
- automatisches Update 88, 90
- manuelles Update 84, 88

Datenverwaltung
- Backup 96
- Quarantäne 93

I

Importieren / Exportieren von Programmeinstellungen 49
Installation
- benutzerdefiniert 23
- Standard 22

L

Lizenz 26

N

Netzwerk
- Proxyserver 91

P

Programm aktivieren
- Testversion 30

Programm mithilfe
- der Schlüsseldatei aktivieren 31
- des Aktivierungscodes aktivieren 30

Programmhauptfenster 34
Prüfungsbereich 72

Q

Quarantäne 93

S

Schädliche Programme 52
Schlüsseldatei 29, 31
Schutzbereich 52
Sicherheitsassistent 34, 44, 45
Sicherheitsstufe
  Datei-Anti-Virus 60
  Virensuche 74
Standardinstallation 22
Start
  Aufgaben zur Virensuche 69
  Autostartmodus des Programms 41

U

Update
  Dateien in der Quarantäne untersuchen 95
  manueller Start 84
  Proxyserver 91
  Rollback zum vorherigen Update 85
  Start nach Zeitplan 90
  Statistik 91
  Updateobjekt 88
  Updatequelle 89
Updateaufgabe starten 84
Updatequelle 86, 89

V

Vertrauenswürdige Zone
  Ausnahmeregel 53
Viren 52
Virensuche 68
  Arbeitsstatistik 81
  heuristische Analyse 76
  Liste der Untersuchungsobjekte 72
  Prüfung von zusammengesetzten Dateien 76
  Sicherheitsstufe 74
  Start nach Zeitplan 78
  Suchoptimierung 76
  Suchtechnologie 76
  Wiederherstellung der Standardparameter 80

W

Wiederherstellung des Objekts 51, 94, 97